Cybersecurity Is a Risky Business

Speakers

Ryan Burns, MLIS
Cyber Risk Services Manager
Texas Municipal League Risk Pool
1821 Rutherford Lane, Suite 100
Austin, Texas 78754
(512) 491-2300 | www.tmlirp.org

TML
INTERGOVERNMENTAL RISK POOL
Partnering with Texas Local Governments Since 1974

Will Trevino
Legal Counsel
Texas Municipal League
1821 Rutherford Lane, Suite 400
Austin, Texas 78754
(512) 231-7400 | www.tml.org

TML
TEXAS
MUNICIPAL LEAGUE

Will Trevino

Will Trevino is the newest member of the Texas Municipal League's legal staff. Will graduated from Texas A&M University in 2004 with a degree in Psychology. In 2007, he received his law degree from Texas Southern University Thurgood Marshall School of Law and received his master of laws from Western New England School of Law in 2011. He is currently enrolled in Baylor University's Hankamer School of Business MBA program with a concentration in cyber security.

Will is the 2018 recipient of the Rising Advocate in Government Law presented by the State Bar of Texas Government Law Section to recognize an outstanding government lawyer who has provided exemplary service to the profession and the public.

Will has worked with cities for more than twelve years now. He provided legal services to cities in both his private practice work and as an in-house attorney for the City of Fort Worth. He is also a council member of the State Bar of Texas Computer Law & Technology Council.

Ryan Burns

Ryan Burns is the Cyber Risk Services Manager for the TML Risk Pool. He has over 16 years of experience working either with or working for public entities in Texas. He joined the TML Risk Pool in 2015 and previously worked in the software/hardware/IT space with local governments as well as in municipal law enforcement. He received his Bachelor of Science degree in Criminal Justice from Sam Houston State University.

Acknowledgements

We wanted to recognize the research and work of Dallas Assistant City Attorney, Lisa Mares, on the first version of this paper prepared for the 2016 TCAA Summer Conference. With her gracious permission, she has allowed us to update and present this paper. Any inaccuracies, misspellings or grammatical errors should not be attributed to her. Once again, thank you Lisa.

TABLE OF CONTENTS

I. Introduction 1

II. Breach of Public Data 1

III. Costs of Data Breach 2

IV. Regulatory Framework 5

A. Texas Laws 6

1. The Identity Theft Enforcement and Protection Act 6

a. Definition of Sensitive Personal Information 6

b. Definition of Breach 7

c. Breach Notification Requirements 8

d. Enforcement 9

2. Texas Medical Records Privacy Act 9

a. Definition of Covered Entity 10

b. Definition of Protected Health Information and Individually Identifiable Health Information 11

c. Definition of Breach 11

d. Breach Notification Requirements 12

e. Additional Requirements 12

f. Exceptions 13

g. Enforcement 14

3. Texas Motor Vehicle Records Disclosure Act 15

a. Definition of Personal Information 15

b. Required or Permitted Disclosure of Personal Information 16

c. Redisclosure of Personal Information 16

d. Enforcement 16

e. Administrative Regulations 17

4. Other State Laws 17

a. Social Security Numbers held by Municipally Owned Utility 18

b. Identifying Financial Information 19

c. Biometric Identifiers 19
d. Crime Victim Information....20
5. Criminal Enforcement....20
B. Federal Laws and Industry Standards....20
1. Health Information Portability and Accountability Act....20
2. Privacy Act of 1974....23
3. Driver's Privacy Protection Act....23
4. Federal Tax Information....23
5. Data Security Standard....23
V. Litigation....24
VI. Conclusion....26

APPENDIX

Summary of the Identity Theft Enforcement and Protection Act and Related Statutes……A

Summary of the Texas Medical Records Privacy Act and Related State Laws, Federal Laws, and Regulations……...B

Cybersecurity Terminology (DIR)……C

Preparing for a Cyber Incident - An Introductory Guide (USSS)……D

Incident Response Template (DIR)……...E

Preparing for a Cyber Incident - A Guide to Ransomware (USSS)……..F

Ransomware Guide (CISA/MS-ISAC)……G

I. INTRODUCTION

Federal, state and local governments hold a wide variety of data about businesses and individuals.[1] The types of data held by public entities range from intellectual property and trade secrets found in bidding documents to financial information submitted in tax and business records. Public entities also maintain an abundance - in amount and assortment - of personal information. For instance, public entities maintain sensitive health information found in employment and ambulatory medical records to personal criminal history record information from police records, to motor vehicle information acquired by traffic citations.[2] Public entities acquire data in various ways, such as while carrying out governmental functions for law enforcement or fire prevention purposes. Individuals also supply personal information to public entities as job applicants, employees or to obtain a government benefit. Furthermore, private entities share information with public entities pursuant to regulatory disclosures, the procurement process, or data sharing agreements.[3]

Some legal scholars argue that a public entity has a "heightened" duty to safeguard business and personal information that is acquired.[4] This paper discusses a city's legal obligations to protect the personally identifiable information it acquires from unauthorized access or disclosure, as well as ensure that such information is accurate, and is intended to be a resource for city attorneys and outside counsel who advise cities how to safeguard the integrity, confidentiality and storage of personal data. To that end, this paper is organized as follows: Part II discusses data acquired by public entities; Part III of this paper briefly discusses direct and indirect costs of a data breach; Part IV provides an overview of state laws regulating sensitive personal information and protected health information held by public entities, select federal laws that regulate the disclosure of individually identifiable information, and industry standards that regulate the collection of information in connection with credit card transactions; Part V addresses barriers to establishing standing in data privacy litigation, efforts to establish standing solely via a statutory violation, and recent class actions litigation against the federal government due to a massive data breach.

II. BREACH OF PUBLIC DATA

Records and data held by public entities ("public data") are at risk for breach. In general, a "breach" is defined as "an event in which an individual's name and a medical record, and/or financial record or debit card is potentially at risk either in electronic or paper format" due to accidental or deliberate unauthorized disclosure.[5] There is a multitude of ways that sensitive data can be disclosed without authorization. Data is unintentionally disclosed when records, portable devices, or computers are lost or improperly discarded, or when an individual

[1] A. Michael Froomkin, *Government Data Breaches*, 24 Berkeley Tech L.J. 1019, 1022 (2009).

[2] *See id.*; Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 439 (2009); U.S. Gen. Accounting Office, GAO-04-548, Data Mining: Federal Efforts Cover a Wide Range of Uses (2004) [hereinafter, GAO, DATA MINING]; Paul Lipman, *Critical Challenges to State and Local Government Cybersecurity Efforts* (Industry Perspective), Government Technology, ¶ 4 (2015), http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html.

[3] *See* Froomkin, *supra* note 1, at 1019, 1022; Cate, *supra* note 2; *see also* GAO, Data Mining, *supra* note 2.

[4] *See* Froomkin, *supra* note 1.

[5] Ponemon Institute, *2020 Costs of Data Breach Study: United States* (2020) [hereinafter Ponemon, *Costs of Data Breach*].

inadvertently emails records to the wrong person or posts records on a website.[6] Data can also be deliberately accessed without authorization via theft, fraud or hacking.[7] As observed by Paul Lipman, former CEO of iSheriff (formerly Internet Sheriff), "[t]he massive amount of valuable data housed by state and local agencies is an attractive target for cybercriminals seeking financial gain."[8] Yet, when compared to the cybersecurity efforts of 17 other major industries, public entities ranked at the bottom of major industries, ranking below information services, financial services, transportation, and healthcare.[9]

Data that is deliberately accessed without authorization may not necessarily be used for financial gain. There has been an increase in using targeted cyber-attacks in the form of cyber espionage or hacktivism. Cyber espionage is used by "digital intelligence agents [who] co-opt surveillance systems, track government employees, and exfiltrate documents for strategic advantage."[10] Cyber espionage is a tool that is usually used by, or on behalf of, government actors.[11] Of the organizations that have experienced a cyber espionage incident impacting the confidentiality, integrity or availability of its data, organizations that fall within the public sector are the most targeted.[12] Likened to protests or civil disobedience, the term "hacktivism" refers to computer hacking for a political purpose or to influence action or a social cause, such as free speech, human rights or information access.[13] Techniques used by so-called hacktivists include defacing or parodying websites, redirecting URLs, denial-of-service attacks, stealing information, virtual sit-ins, and virtual sabotage.[14] These types of attacks can result in a great deal of economic harm to an individual, a business, and can even threaten critical infrastructure.[15]

Cyber espionage is not the only thing to worry about. Most recently, local governments have seen an uptick in ransomware attacks.[16] Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.[17] Once a computer or system is infiltrated, cybercriminals demand ransom in exchange for a decryption key or to prevent release of information by the cybercriminal – a form of modern-day blackmail.[18] In recent months,

---

[6] Privacy Rights Clearinghouse, *Chronology of Data Breaches* (2021), https://privacyrights.org/data-breaches [hereinafter Privacy Rights, *Chronology of Data Breaches*].
[7] *Id.*; Ponemon, *Costs of Data Breach*, *supra* note 5, at 8.
[8] Lipman, *supra* note 2, at ¶ 4.
[9] SecurityScorecard R&D Department, *2016 U.S. Government Cybersecurity Report* 3 (2016), http://info.securityscorecard.com/2016-us-government-cybersecurity-report (Paul Lipman is now President at Quantum Computing at ColdQuanta).
[10] McAfee Labs, *2016 Threats Predictions* 17, 35 (2015), http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf.
[11] Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 1, A-1, B-1 thru B-3 (2011).
[12] Verizon Enterprises, *2016 Data Breach Investigations Report* (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/.
[13] McAfee Labs, *supra* note 10.
[14] Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation 3, 6, 104, 124 (September 2004) (unpublished Ph.D. thesis, Harvard University) (*available at* http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf).
[15] Verizon Enterprises, *supra* note 12, at 80.
[16] Texas Department of Information Resources, *Update on Texas Local Government Ransomware Attack* (2021), https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213.
[17] CISA, *Stop Ransomware: Resources* (2021), https://www.cisa.gov/stopransomware/resources.
[18] *Id.*

ransomware has dominated the headlines, but incidents among the Nation's state, local, and territorial government entities and critical infrastructure organizations have been growing for years.[19] Many cities have paid the ransom out of the taxpayers' coffers, while others have relied on cyber insurance to pay the ransom.[20] Legislation was introduced in the 87th Texas legislative regular session that would have prohibited cities, and other political subdivisions, from paying a ransom.[21] The bill was referred to State Affairs and never made it out of committee. However, it is one bill that may resurface in future legislative sessions.

III. COSTS OF DATA BREACH

Whether public or private, an entity faces significant costs when responding to a breach incident. The expenses faced by an entity include the costs to detect, recover, investigate, and manage incident response. Additional expenses incurred by the breached entity include indirect costs to mitigate financial loss faced by customers and minimize disruptions to operations.[22] For public or private entities located in the United States, the cost of a single data breach incident is estimated at $8.64 million or an average of $146 per individual record that was lost or stolen.[23] The public sector has the lowest average cost of a data breach when compared to other industries. For instance, the average cost of a data breach for the public sector was $1.08 million, compared to $7.13 million for the healthcare industry.[24] These figures beg the question, "*why the difference?*" The answer stems, in part, from the types of services offered by the public and private sector. Much of the personal or business information that a public entity collects is acquired pursuant to a legal requirement, in connection with a government benefit, or due to a licensing condition or regulatory compliance.[25] The health, financial, technology, and service industries likely experience higher indirect costs due to a loss in customers, while the public sector experiences lower indirect costs due to customer loss because government benefit recipients and regulated entities are parties to an involuntary transaction, and have few or no alternatives to dealing with the breached public entity.[26]

The answer to the inquiry regarding why a breached public entity faces lower costs than a breached private entity also stems from how state and federal governments self-regulate with respect to the data that governments create, collect and access.[27] Many state and federal laws exempt public data breaches from civil and criminal penalties. Even when a public entity is subject to penalties, they are only imposed if the public entity's conduct is egregious. One of the first public entities to enter into a settlement agreement due to a violation of the Health Insurance Portability and Accountability Act ("HIPAA") violation is Skagit County, Washington in 2014.

The Skagit County health department improperly posted the medical payment records of

---

[19] NPR, *22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault* (2019), https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault.
[20] Business Insider, *8 cities that have been crippled by cyberattacks — and what they did to fight them* (2020), https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1#baltimore-maryland-2.
[21] TEX. H.B. 3892, 87th. LEG., R.S. (2021).
[22] Ponemon, *Costs of Data Breach*, *supra* note 5, at 72.
[23] Ponemon, *Costs of Data Breach*, *supra* note 5, at 12.
[24] *Id*. at 25.
[25] Froomkin, *supra* note 1, at 1019, 1023-25.
[26] Ponemon, *Costs of Data Breach*, *supra* note 5, at 25; Froomkin, *supra* note 1, at 1019, 1025.
[27] Cate, *supra* note 2, at fn. 7, 435, 437-38.

1,600 patients on a public web server. The records contained patient first and last names, the health service received, medical procedure and diagnostic codes, the date of payment, and in cases where a patient paid with a credit or debit card, the last 4 digits of the card.[28] Additional violations noted by the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") included non-compliance with the Breach Notification Rule and the Security Rule by failing to notify affected persons of the breach, to maintain security policy and procedures, and to train personnel to maintain the privacy and security of protected health information.[29] The County entered into a settlement agreement of $215,000 and a corrective action plan with the OCR. OCR noted that "[t]his case marks the first settlement with a county government and sends a strong message about the importance of HIPAA compliance to local and county governments, regardless of size."[30] The OCR indicated that state and local governments are not immune from future enforcement actions and that such "agencies need to adopt a meaningful compliance program to ensure the privacy and security of patients' information."[31]

Despite warnings of the necessity to secure individually identifiable data, more than 293 million records held by public entities are estimated to have been lost or breached since 2005.[32] Several recently discovered breaches involving data held by the Office of Personnel Management ("OPM") have put millions of individuals at risk of identity theft.[33] In June of 2015, the OPM, which maintains records for current, former, and prospective federal employees, notified approximately 4 million federal employees that the computer systems of a background investigative services contractor had been hacked.[34] The OPM initially estimated that the personally identifiable information of 4 million federal employees may have been stolen, giving the hackers access to biometric fingerprints; residency and educational history; employment history; family information and other personal information; health, criminal and financial history; and other details, such as foreign trips taken, names of neighbors and close friends, and more.[35] Recent reports indicate that the background investigative and personal data of two of OPM's contractors - KeyPoint and U.S. Investigations Services - were hacked, affecting approximately 25.7 million records belonging to 22.1 million current, former and prospective federal employees, as well as their spouses or partners.[36] To date, the expenses incurred by the federal

---

[28] Skagit County, Washington, Notice of HIPAA Breach (*available at* http://www.skagitcounty.net/Departments/Home/hipaa.htm).

[29] U.S. Dep't of Health & Human Services, Resolution Agreement and Corrective Action Plan with Skagit County, Washington 1-2 (March 6, 2014) (*available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/skagit-county-settlement-agreement.pdf).

[30] Press Release, U.S. Dep't of Health & Human Services, County Government Settles Potential HIPAA Violations, ¶ 2 (March 7, 2014) (*available at* http://www.hhs.gov/about/news/2014/03/07/county-government-settles-potential-hipaa-violations.html).

[31] *Id*.

[32] Privacy Rights, *Chronology of Data Breaches, supra* note 5.

[33] *Id*. (A search for breaches disclosed during the last two years indicates that breaches have been reported by the following federal agencies: the Federal Deposit Insurance Corporation, the Internal Revenue Service, the U.S. State Department, the U.S. Weather Service, the U.S. Postal Service, and the Department of Veterans Affairs).

[34] David Bisson, *The OPM Breach: Timeline of a Hack*, The State of Security, July 10, 2015, at http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

[35] Press Release, U.S. Office of Personnel Management, OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats (July 9, 2015) (*available at* https://www.opm.gov/news/releases/2015/07/opm- announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/).

[36] Jedidiah Bracy, *21.5 Million Breached In Second OPM Hack; Director Resigns*, Privacy Tech, ¶ 2 (July 10,

government in connection with these breaches include temporary credit monitoring services, fraud protection, and identity theft insurance for roughly 28 million individuals. In credit monitoring services alone, the federal government will pay at least $133 million; the total figure might eventually reach $1 billion.[37] The true cost of the massive OPM date breach remains to be seen since multiple lawsuits have been filed by federal employees.[38] These lawsuits are discussed in further details in Part V, *infra*.

IV. REGULATORY FRAMEWORK

In the United States, unlike other countries, lawmakers have not enacted a uniform law that protects data. Instead, the collection, storage, release, or destruction of data is regulated on both the state and federal level, and such regulations are primarily enforced by industry, *e.g.*, business industry, health industry, financial services industry, or public utilities[39]; activity, *e.g.*, electronic communication, electronic marketing, surveillance, conducting background checks the type of data, *e.g.*, cancer, genetic, HIV/AIDS, sexual assault, mental health, immunizations, federal tax, customer records of a government-operated utility, or government benefit recipient information[40]; or the status of the individual, *e.g.*, a minor, an elected official, or a government employee.[41] This piecemeal approach is why the legislative framework for the protection of individually identifying information is often compared to a patchwork quilt.[42] Consequently, there are numerous state and federal laws that regulate data privacy with different requirements depending on the regulated industry, entity, activity or status of the individual.

2015), https://iapp.org/news/a/21-5-million-breached-in-second-opm-hack/.

[37] CSO, *The OPM hack explained: Bad security practices meet China's Captain America* (2020), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[38] Zach Noble, *Full dollar cost of OPM breach still a giant unknown*, FCW, ¶ 3, 5 (September 2015) (*available at* https://fcw.com/articles/2015/09/10/opm-breach-cost.aspx).

[39] Lisa J. Sotto & Aaron P. Simpson, *Data Protection & Privacy 2015, United States*, *in* Getting The Deal Through 208 (Rosemary P. Jay, cont. ed., 2014); *see also* Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, The New York Times (March 30, 2013).

[40] *See, generally*, TEX. HEALTH & SAFETY CODE §82.009(a) (relating to confidentiality of cancer reports, records and information obtained the Texas Board of Health); Genetic Information Nondiscrimination Act of 2008 ("GINA") Pub. L. No. 110-233, TEX. INS. CODE §546.102, TEX. LABOR CODE §21.403 and TEX. OCC. CODE §58.102 (relating to confidentiality of records containing genetic information); TEX. HEALTH & SAFETY CODE §81.103(a) (relating to confidentiality of HIV/AIDS test results); TEX. GOV'T CODE §§420.010 and 420.071 (relating to identification of, and communications with, sexual assault victims); TEX. HEALTH & SAFETY CODE §611.002(a) (relating to communications between a patient and professional for diagnosis, evaluation or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction); TEX. HEALTH & SAFETY CODE §161.0073 (relating to confidentiality of immunization records); TEX. UTIL. CODE §182.052 (relating to confidentiality of customer records held by a government-operated utility); 26 U.S.C. § 6103(a) (relating to confidentiality of federal tax return and tax return information); 7 C.F.R. §272; 45 C.F.R. §205.50; 42 C.F.R. §§ 431.300, 457.1110 (concerning recipients of government benefits, such as Medicaid, the Supplemental Nutrition Assistance Program, Temporary Assistance for Needy Families, or the Children's Health Insurance Program by the Health and Human Services Commission, its designee(s), third party(ies), or business associates).

[41] *See, e.g.*, TEX. ALC. BEV. CODE § 106.117(d), TEX. CODE OF CRIM. PROC. arts. 44.2811, 45.0217(a), 63.015(b), 63.017; TEX. EDUC. CODE § 25.002(b); TEX. FAM. CODE §§33.002(f), 33.003(k), (*l*) and (*l*-2), 33.004(c), 54.033(f), 54.04(w)(3), 58.005, 58.007(b) and (c), 58.00711(b), 58.0072, 58.106, 58.307 and 85.007; TEX. GOV'T CODE § 422.004; TEX. OCC. CODE §159.005 (relating to confidentiality or release of information involving a minor, child or juvenile).

[42] *See, e.g.*, Sotto & Simpson, *supra* note 39, at 208.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.[43] Some states impose civil penalties or authorize a private right of action against a public entity that fails to safeguard the privacy, security or integrity of identifying information.[44] In addition, the definition of personally identifiable information varies depending on the applicable law or regulation. In the security breach notification law context, for example, personal identifiable information generally includes an individual's name in conjunction with the individual's Social Security number, driver's license number, or bank account number.[45]

A. Texas Laws

In Texas, a local government can face civil penalties if it does not comply with state breach notification laws. The key state laws that regulate the disclosure of identifiable information owned or maintained by a local government are (1) The Identity Theft Enforcement and Protection Act (the "ITEPA"); (2) The Texas Medical Records Privacy Act ("TMRPA"); and (3) other state laws that protect social security numbers, biometric identifiers, and crime victim information. The key terms under these laws are "sensitive personal information" and "protected health information." This section of the paper provides an overview of Texas laws that regulate the collection, storage, release, or destruction of data containing certain identifiable information held by a local government.[46]

1. The Identity Theft Enforcement and Protection Act

The ITEPA imposes a duty on businesses to protect and safeguard sensitive personal information and requires the notification of an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information. While the ITEPA does not expressly apply to local governments, Chapter 205 of the Local Government Code incorporates key provisions of the ITEPA. Thus, a local government must comply with the breach notification requirements of the ITEPA.[47]

a. Definition of Sensitive Personal Information

The ITEPA covers a business that collects or maintains "sensitive personal information" of Texas residents in its regular course of business.[48] The ITEPA broadly defines sensitive personal information to cover an individual's first name or first initial and last name in combination with any one or more of the following unencrypted pieces of information:

---

[43] National Conference of State Legislatures, *Security Breach Notification Laws* (April 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [hereinafter NCSL, *Breach Notification Laws*].

[44] *See, e.g.*, The Identity Theft Enforcement and Protection Act, codified at TEX. BUS. & COM. CODE §§ 521.001; 521.152 and The Texas Medical Records Privacy Act, codified at TEX. HEALTH & SAFETY CODE §§ 181.001 – 181.207.

[45] NCSL, *Breach Notification Laws*, *supra* note 43.

[46] This paper uses the term "identifiable information" to generally refer to all types of information that identifies an individual, whether financial, medical, criminal, or consumer records are involved. The regulation of a local government that collects and maintains information related to critical infrastructure is beyond the scope of this paper.

[47] TEX. LOC. GOV'T CODE ANN. § 205.010.

[48] TEX. BUS. & COM. CODE § 521.002(a)(2).

- Social Security number;
- Driver's license number or government-issued identification number; and
- Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.[49]

Sensitive personal information also covers information that identifies an individual and relates to (i) the physical or mental health or condition of the individual, (ii) the provision of health care to the individual, or (iii) the payment for the provision of health care to the individual.[50] However, sensitive personal information does not include "publicly available information that is lawfully made available to the public from the federal government or a state or local government."[51]

ITEPA requires a covered business to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure of any sensitive personal information collected or maintained by the business in the regular course of business."[52] Additionally, covered businesses are required to destroy or arrange for the destruction of records that contain sensitive personal information by (1) shredding, (2) erasing, or (3) otherwise modifying the sensitive personal information contained in the records in a manner "to make the [personal] information unreadable or indecipherable through any means."[53] State law does not impose a similar duty on local governments. However, a duty to implement procedures to prevent the unlawful use or disclosure of sensitive personal information may be imposed on a local government if the local government uses, stores or exchanges medical information. A local government that uses, stores or exchanges medical information may be a "covered entity" under HIPAA or TMRPA.

b. Definition of Breach

ITEPA defines a "breach of system security" as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a business, including data that is encrypted if the person accessing the data has the key required to decrypt the data. However, good faith acquisition of sensitive personal information by an employee or agent of the person is not a breach unless the information is used or disclosed, whether by the employee, the agent, or any other individual, in an unauthorized manner.[54]

Certain local governments must comply with provisions of the ITEPA. Specifically, a local government that owns, licenses, or maintains computerized data that includes sensitive personal information must comply with the notification requirements of ITEPA to the same extent as a person who conducts business in Texas in the event of a breach of system security.[55]

---

[49] *Id*.
[50] TEX. BUS. & COM. CODE § 521.002(a)(2)(B).
[51] *Id*. § 521.002(b).
[52] *Id*. § 521.052(a).
[53] *Id*. § 521.052(b).
[54] *Id*. § 521.053(a).
[55] TEX. LOC. GOV'T CODE § 205.010(b).

Similarly, a state agency that owns, licenses, or maintains computerized data that includes sensitive personal information must comply with the notification requirements of ITEPA in the event of a breach of system security.[56]

c. Breach Notification Requirements

A business, local government or state agency that owns, licenses, or maintains computerized data that includes sensitive personal information must disclose a breach after discovering or receiving notice of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The required disclosure must be made without unreasonable delay, and in each case not later than the 60th day after the date on which the entity determines that the breach occurred, unless a law enforcement agency requests a delay in notification to avoid compromising an ongoing investigation or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[57] If the individual whose sensitive personal information was breached is a resident of another state, the required notice may either be provided under that state's law or under Texas law.[58] If an affected individual resides in a state without a data breach notification statute, the individual must be notified in accordance with Texas law.

A business, local government, or state agency may provide the required notice via either: (i) written notice mailed to the last known address of the individual; or (ii) electronic notice, only if the notice is provided in accordance with the federal Electronic Records and Signatures in Commerce Act.[59] If a business, local government or state agency is required by ITEPA to notify more than 10,000 individuals of a breach of system security at one time, the business, local government or state agency must also notify, without unreasonable delay, each consumer reporting agency that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.[60]

Alternatively, if the business, local government or state agency demonstrates that the cost of providing notice would exceed $250,000, there are more than 500,000 affected individuals, or the business, local government or state agency does not have sufficient contact information for the affected individuals, the notice may be given by:

- E-mail if maintained for the affected individuals;
- Conspicuous posting of the notice on the business, local government or state agency's website; or
- Notice published in or broadcast on major statewide media.[61]

A business, local government or state agency that maintains separate notification procedures as part of an information security policy for the treatment of sensitive personal information may provide the required notice in accordance with the notification methods of such a policy, but it

[56] TEX. GOV'T CODE § 2054.1125(b).
[57] TEX. BUS. & COM. CODE § 521.053(b).
[58] *Id.* § 521.053(b-1).
[59] TEX. BUS. & COM. CODE § 521.053(e); *see also* 15 U.S.C. § 7001.
[60] TEX. BUS. & COM. CODE § 521.053(h).
[61] *Id.* § 521.053(f).

must adhere to the timing requirements for notice under ITEPA.[62]

d. Enforcement

The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation.[63] A person who fails to take reasonable action to comply with the notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach.[64] These provisions, arguably, do not apply to a local government.[65]

If it appears to the Attorney General that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the Attorney General may bring an action against the person for a temporary restraining order or by a permanent or temporary injunction. These provisions, arguably, do apply to a local government.[66] A violation of ITEPA is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.[67] Recently adopted legislation, that becomes effective September 1, 2021, requires notification to be sent to the attorney general regarding a breach of system security under Business and Commerce Code sec. 521.053 to include the number of affected residents that had been sent a disclosure of the breach by mail or other direct method of communication at the time of notification.[68] The attorney general would have to then post on the attorney general's website a comprehensive listing of all received notifications of security system breaches, and the listing would have to be updated within 30 days after notification of a new breach of system security was received.[69] Sensitive personal information and other confidential information that had been reported to the attorney general under sec. 521.053 would be excluded from the listing.[70]

2. Texas Medical Records Privacy Act

The TMRPA, in some respects, provides more protection for individual privacy than its federal counterpart, Title 2 of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, the Privacy Rule, the Security Rule, the Enforcement Rule, and the Omnibus Rule (hereinafter referred to collectively as "HIPAA"). TMRPA incorporates by reference a few key terms of HIPAA and the Privacy Rule.[71] TMRPA provides additional protections by defining key terms more broadly, establishing additional protections for individuals, and imposing stiffer

[62] *Id*. § 521.053(g).
[63] *Id*. § 521.151(a).
[64] *Id*. § 521.151(a-1).
[65] *Id*. § 521.151(a) and (a-1).
[66] *Id*. § 521.151(b).
[67] *Id*. § 521.152; see also § 17.45.
[68] Certain Notifications Required Following a Breach of Security of Computerized Data, 2021 Tex. Sess. Law Serv. Ch. 496 (H.B. 3746) (VERNON'S).
[69] *Id.*
[70] *Id.*
[71] The regulations referred to as The Privacy Standards are located at 45 C.F.R. Part 160, 162, and 164, Subparts A and E, as amended by HITECH.

penalties for non-compliance.[72]

One key difference between HIPAA and TMRPA is that Texas law imposes a broader definition of a "covered entity," thereby regulating additional entities beyond HIPAA. A local government that merely uses, stores or exchanges medical information is likely a "covered entity" under TMRPA. In this paper, these types of local governments are referred to as a TMRPA covered entity. It is important to note that a local government that is subject to TMRPA, but that is not subject to HIPAA because it is not a health plan, health provider or health information exchange, only needs to comply with TMRPA and does not need to also comply with HIPAA, HITECH and related administrative regulations.[73]

Another key difference is that state law does not impose any breach notification requirements on a TMRPA covered entity. That is, in the event of a breach of protected health information, a TMRPA covered entity does not need to notify an affected individual unless the breach involves computerized records that indicate the physical or mental health or condition of an individual, the provision of health care to the individual, or the payment of health care services because the breach of this type of medical information is regulated by ITEPA. A local government that is a covered entity under HIPAA because it is a health plan, health provider, or health information exchange, should consult Part IV.B.1. of this paper, which summarizes federal regulations regarding data security for a local government that is regulated as a covered entity under HIPAA.[74] In this paper, these types of local governments are referred to as a HIPAA covered entity.

a. Definition of Covered Entity

As indicated, TMRPA defines "covered entity" broadly enough to include many entities that are not regulated under HIPAA. TMRPA defines a covered entity as any person who for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis:

- Assembles, collects, analyzes, uses, evaluates, stores, or transmits protected health information;
- Comes into possession of protected health information; or
- Obtains or stores protected health information under TMRPA.[75]

By definition, a covered entity expressly includes a health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, or health care provider, or person that maintains an Internet site.[76] A TMRPA covered entity also includes an employee, agent, or contractor of a covered entity if the employee, agent, or

[72] Cheryl Camin Murray, *Don't Mess with Texas – A Summary of State Laws Concerning Health Information*, HEALTHCARE DAILY (May 1, 2013).
[73] *New Developments in Safeguarding Protected Health Information During 2014* Submitted to the House Public Health Committee and the Senate Health and Human Services Committee by the Health and Human Services Commission (December 2014).
[74] 45 C.F.R. § 160.103.
[75] TEX. HEALTH & SAFETY CODE §181.001(b)(2)(A)-(C).
[76] *Id*. § 181.001(b)(2)(A).

contractor creates, receives, obtains, maintains, uses, or transmits protected health information.[77]

b. Definition of Protected Health Information and Individually Identifiable Health Information

TMRPA incorporates definitions from HIPAA and the Privacy Standards for terms that are referenced in TMRPA but that are not expressly defined.[78] Protected health information is one such term. Thus, for purposes of TMRPA, "protected health information" means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any form or medium by a covered entity or its business associate.[79] Protected health information does not include "individually identifiable health information": (i) in education records covered by the Family Educational Rights and Privacy Act ("FERPA") that are available to parents or education records for those over age 18 or in college; or (ii) in employment records held by a covered entity in its role as employer unless the employer's activities involve the re-identification, marketing, the sale, or the electronic disclosure of protected health information.[80] For a governmental unit that is a TMRPA covered entity, an individual's protected health information also includes information that reflects that an individual received health care from a governmental unit unless that information is subject to disclosure pursuant to Chapter 552 of the Government Code.[81]

Individually identifiable health information is another term that is referenced, but not defined, in TMRPA. Thus, a local government must look to HIPAA and the Privacy Standards for the definition of this term. Under the Privacy Standards, individually identifiable health information is a type of information collected from an individual, including demographic information that either identifies an individual or can be used to identify the individual and relates to:

- The past, present, or future physical or mental health or condition of an individual;
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual.[82]

c. Definition of Breach

Recall that TMRPA incorporates definitions from HIPAA and the Privacy Standards for terms that are referenced in TMRPA, but that are not expressly defined. TMRPA does not reference the term "breach," therefore, TMRPA does not incorporate the definition of breach from HIPAA or the Privacy Standards. Even though TMRPA does not impose any breach notification requirements, a local government that is a TMRPA covered entity is subject to data breach notification requirements. A comparison of the definition of individually identifiable

[77] *Id*. § 181.001(b)(2)(D).
[78] *Id*. § 181.001(a).
[79] 45 C.F.R. § 160.103.
[80] TEX. HEALTH & SAFETY CODE §§ 181.051, 181.151-181.154.
[81] *Id*. §181.006.
[82] 45 C.F.R. § 160.103.

health information and sensitive personal information shows that the definition of individually identifiable information is subsumed by the definition of sensitive personal information to the extent the information is maintained as computerized data. Under the ITEPA, "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a local government, including data that is encrypted if the person who acquires the data has the key to decrypt the data. A local government that owns, licenses, or maintains computerized data that identifies an individual and relates to: (1) the physical or mental health or condition of the individual; (2) the provision of health care to the individual; or (3) the payment for the provision of health care to the individual since such activities are regulated by, and thus fall under the umbrella of, the ITEPA.[83] To be clear, a local government that experiences a breach of computerized data that involves either sensitive personal information or individually identifiable information that it owns, licenses, or maintains, must comply with the breach notification requirements of ITEPA.

d. Breach Notification Requirements

A local government that is a TMRPA covered entity must comply with the breach notification requirements under ITEPA if it is a TMRPA covered entity and experiences a breach of system security that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or the payment for the provision of health care to the individual such that it compromises the security, confidentiality, or integrity of the information.[84]

e. Additional Requirements

Aside from complying with breach notification requirements, a TMRPA covered entity must comply with regulations that: (i) restrict the disclosure of protected health information in electronic format; (ii) restrict the use of protected health information for marketing purposes; (iii) prohibit the sale of protected health information; and (iv) mandate certain employee training. A TMRPA covered entity may not electronically disclose an individual's or employee's protected health information unless it provides both notice and authorization from the individual or the individual's legally authorized representative for *each* disclosure. A TMRPA covered entity may provide general notice by:

- Posting a written notice in the covered entity's place of business;
- Posting a notice on the covered entity's Internet website; or
- Posting a notice in any other place where individuals whose protected health information is subject to electronic disclosure are likely to see the notice.

Authorization is not required if the disclosure is authorized or required by state or federal law. If the disclosure is not authorized or required by law, a separate authorization is required for every disclosure of protected health information in electronic format.

83 *See supra* Part IV.A.1.
84 TEX. LOC. GOV'T CODE § 205.010; TEX. BUS. & COM. CODE §§ 521.002(2), 521.053.

In addition, a TMRPA covered entity may not use or disclose protected health information for marketing purposes without first obtaining consent or authorization from the individual.[85] Written communications must explain the recipient's right to removal from the mailing list, and removal must be accomplished by TMRPA covered entity within 45 days after the receipt of the request.[86] TMRPA also imposes a blanket prohibition on selling protected health information. That is, a TMRPA covered entity may not disclose an individual's protected health information to anyone in exchange for direct or indirect remuneration.[87]

Finally, a TMRPA covered entity must train its employees on state and federal laws regarding the entity's use, storage or exchange of protected health information within 90 days after the employee is hired and within one year of a material change in law concerning protected health information. Each employee must sign a statement verifying the employee's training. TMRPA covered entity must maintain these signed statements for six years.[88]

f. Exceptions

TMRPA exempts many types of records from its regulations. What follows are the exceptions that are most likely to apply to a local government entity – exceptions that apply to records held as an employer, workers compensation records, certain medical records regarding juveniles, and certain records regarding crime victims. For information held by a local government in its scope as an employer, TMRPA imposes additional regulations on a TMRPA covered entity. Unlike HIPAA, TMRPA only provides for a partial exception for employer records. If an employer re-identifies the protected health information of its employees, markets the protected health information of its employees, sells protected health information of its employees, or electronically discloses the protected health information of its employees, it must comply with TMRPA when doing so.[89] However, with respect to workers compensation records, TMRPA does not apply to workers' compensation insurance, a function authorized by Title 5 of the Labor Code, or any person in connection with providing, administering, supporting, or coordinating any of the benefits under a workers' compensation self-insured program.[90] TMRPA also exempts an employee benefit plan and a covered entity or person acting in connection with an employee benefit plan.[91] The important takeaway for city attorneys is that a local government that re-identifies the protected health information of its employees, markets the protected health information of its employees or electronically discloses the protected health information of its employees must do so in accordance with TMRPA. *A local government cannot receive direct or* indirect compensation in exchange for the protected health information of its employees.

With respect to juveniles, TMRPA does not apply to "education records" covered by FERPA or other records accessible by an educational agency, such as law enforcement records created by a law enforcement unit of the educational agency or institution for law enforcement purposes.[92] In addition, TMRPA does not apply to an agency listed or described in Health and

[85] TEX. HEALTH & SAFETY CODE § 181.152.
[86] *Id*. §§ 181.152(b)(2) and (c).
[87] *Id*. § 181.153.
[88] *Id*. § 181.101.
[89] *Id*. §§ 181.051 and 181.151-181.154.
[90] *Id*. § 181.154.
[91] *Id*. § 181.055.
[92] *Id*. § 181.058; 20 U.S.C. § 1232g(a)(4)(B) (excluding certain records held or accessible by an education agency

Safety Code, Section 614.017 that discloses, receives, transfers, or exchanges protected health information related to a special needs offender or a juvenile with a mental impairment in the custody of the agency for purposes of continuity of care and services.[93] Among the many entities listed in Section 614.017, local jails regulated by the Commission on Jail Standards, a municipal or county health department, and a hospital district and a judge with jurisdiction over juvenile or criminal cases are included.[94]

Finally, TMRPA does not apply to certain medical or law enforcement records held by a local government. Specifically, a local government does not have to comply with TMRPA when it creates, maintains or transmits protected health information in connection with providing, administering, supporting, or coordinating benefits regarding compensation to crime victims as provided by Code of Criminal Procedure, Chapter 56, Subchapter B.[95]

g. Enforcement

TMRPA authorizes the Texas Attorney General to institute an action for civil penalties due to TMRPA violations. The civil penalty imposed under TMRPA is capped at:

- $5,000 per violation per year committed negligently;
- $25,000 per violation per year if committed knowingly or intentionally; or
- $250,000 per violation if the covered entity knowingly or intentionally used the protected health information for financial gain.[96]

The total amount of a penalty assessed against a TMRPA covered entity due to a violation that involves the electronic disclosure of protected health information may be reduced and capped at $250,000 annually if the court finds that the disclosure was made to another covered entity for treatment, payment, health care operations, performing an insurance or health maintenance organization function or as otherwise authorized or required by state or federal law only if the court finds that: (i) the disclosed protected health information was encrypted or transmitted using encryption technology designed to protect against improper disclosure; (ii) the recipient of the protected health information did not use or release the protected health information; or (iii) at the time of the disclosure, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of protected health information.[97]

In a proceeding to impose an administrative or civil penalty due to the disclosure of individually identifiable health information, a covered entity may introduce, as mitigating evidence, evidence of the entity's good faith efforts to comply with: (i) state law related to the privacy of individually identifiable health information; or (ii) HIPAA and the Privacy

from the definition of education records).
[93] TEX. HEALTH & SAFETY CODE § 181.055.
[94] *Id*. § 181.057; TEX. HEALTH & SAFETY CODE § 614.017.
[95] *Id*. § 181.059.
[96] *Id*. § 181.201(b).
[97] *Id*. § 181.201(b-1).

Standards.[98] In determining a penalty imposed on a TMRPA covered entity that is licensed by a state agency, a court or state agency must consider the following factors:

- The seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure;
- The covered entity's compliance history;
- Whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose protected health information is involved in the violation;
- Whether the covered entity was certified at the time of the violation under Health & Safety Code, Section 182.108;
- The amount necessary to deter a future violation; and
- The covered entity's efforts to correct the violation.[99]

Unlike the ITEPA, TMRPA does not exempt a local government entity from civil penalties or other enforcement actions. Thus, a local government that uses, stores or exchanges medical information in its scope as an employer must comply with portions of TMRPA and a local government that is a TMRPA covered entity is exposed to significant liability if it violates TMRPA.

3. Motor Vehicle Records Disclosure Act

The MVRDA was to implement the provisions of the federal Driver's Privacy Protection Act ("DPPA"). These laws protect personal information contained in the motor vehicle records. The release and use of all personal information contained in a motor vehicle record is restricted and should be released only as authorized by state or federal law.

a. Definition of Personal Information

The Motor Vehicle Records Disclosure Act ("MVRDA") prohibits the disclosure and use of personal information contained in motor vehicle records unless authorized by the individual or by state or federal law.[100] The law applies to a political subdivision that compiles or maintains motor vehicle records, including the authorized agent or contractor of a political subdivision.[101] The MVRDA defines "personal information" as information that identifies a person, including:

- an individual's photograph or computerized image,
- social security number,
- date of birth,
- driver identification number,
- name,
- address, but not the zip code,
- email address,

[98] *Id*. § 181.205(a).
[99] *Id*. § 181.205(b).
[100] TEX. TRANS. CODE § 730.002.
[101] *Id*. § 730.003(1).

- telephone number, and
- medical or disability information.

The term does not include (i) information about vehicle accidents, driving or equipment-related violations, or driver's license or registration status; or (ii) information contained in an accident report prepared under Transportation Code, Chapter 550 or 601.[102]

b. Required or Permitted Disclosure of Personal Information

Personal information obtained by a political subdivision must be disclosed for use in connection with: (i) motor vehicle or motor vehicle operator safety; (ii) motor vehicle theft; (iii) motor vehicle product alterations, recalls, or advisories; (iv) performance monitoring of motor vehicles, motor vehicle parts, or motor vehicle dealers; (v) motor vehicle market research activities, including survey research; or (vi) removal of non-owner records from the original owner records of motor vehicle manufacturers; (vii) child support enforcement; (viii) enforcement actions by the Texas Workforce Commission; and (ix) voter registration or the administration of elections.[103] In addition, a political subdivision must release personal information to a requestor who is the subject of the information, or if the requestor has written consent from the person who is the subject of the information.[104] A political subdivision may release the (i) name and address; (ii) date of birth; and (ii) driver's license number for a permitted use as specified under Transportation Code, Section 730.007.

c. Redisclosure of Personal Information

Personal information released by a state agency or political subdivision may not be redisclosed, including redisclosure for compensation, unless it is to be used only as permitted by MVRDA. In addition, a recipient of personal information may not redisclose the personal information in an identical or substantially identical format that the state agency or political subdivision disclosed such information to the recipient. A political subdivision, its agent or contractor must require a recipient of personal information to maintain a record of disclosures of redisclosed information to an individual or entity. The record must include the permitted use for which personal information was redisclosed. The record of disclosures and permitted uses must be maintained by the recipient for at least 5 years. Also, the person or entity must provide a copy of the record of disclosures and permitted uses to the political subdivision upon request.[105] Moreover, recent legislation adopted in 2021 now requires an authorized recipient to notify each person who receives personal information from the authorized recipient that the person may not redisclose the personal information to a person who is not an authorized recipient.[106]

d. Enforcement

A violation of a requirement of MVRDA can result in civil and criminal penalties.

[102] *Id*. § 730.003(6).
[103] *Id*. § 730.005.
[104] *Id*. § 730.006.
[105] *Id*. § 730.013.
[106] Texas Consumer Privacy Act Phase I; Creating Criminal Offenses; Increasing the Punishment for an Existing Criminal Offense, 2021 Tex. Sess. Law Serv. Ch. 935 (S.B. 15) (VERNON'S).

Violations include falsifying statements, or knowingly, obtaining, disclosing, or using the information obtained from a motor vehicle record in violation of MVRDA. A person who is convicted of a violation of MVRDA or an administrative regulation adopted by a state agency relating to the terms or conditions for release of personal information is ineligible to receive personal information under Transportation Code, Section 730.007.[107] Additionally, not later than one year after the date of conviction or the court's final determination of a violation under MVRDA, the person must delete from the person's records all personal information received under MVRDA; and may not redisclose personal information received.

A civil or criminal penalty can be imposed on an individual, organization, or entity, who obtains, has access to, uses, releases, or rediscloses motor vehicle information in violation of MVRDA.[108]. Finally, a person convicted of an offense under MVRDA may be punishable by a fine not exceeding $100,000. The state, a state agency, political subdivision, or an authorized agent or contractor of a state agency or political subdivision that compiles or maintains motor vehicle records is exempt from the enforcement provisions.[109]

e. Administrative Regulations

In addition to state law requirements that regulate a political subdivision's disclosure of motor vehicle records, state agencies that sell or provide access to driver records have promulgated administrative regulations that require a written service agreement with a local government when releasing motor vehicle record information.[110] A political subdivision should review agreements entered into with the Texas Department of Public Safety ("DPS") and the Texas Department of Motor Vehicles ("DMV") to determine whether it must comply with any breach notification or privacy requirements in addition to those imposed on political subdivisions via state and federal law. For instance, a standard agreement drafted by DPS requires a political subdivision to notify the agency within two calendar days of any inadvertent or unauthorized release, disclosure, breach, or compromise of driver records. An agency may hold a political subdivision responsible for ensuring that any party to which the political subdivision releases driver record information complies with all federal and state laws that regulate the release of such records. If a state agency determines that an improper disclosure of personal information has been made by any party that directly or indirectly obtained the driver record information from a political subdivision, the agency may terminate the agreement with the political subdivision.[111] If an agreement is terminated due to a violation of a clause or term of the agreement, it cannot enter into a subsequent agreement to obtain driver record information with either agency.[112]

4. Other State Laws

Texas laws also restrict the use or disclosure of other types of information. Provisions of the Business and Commerce Code regulate the disclosure of (i) social security numbers to

[107] *Id*. § 730.016.
[108] *Id*. §§ 730.013 and 730.015.
[109] *Id.* § 730.003(5).
[110] 37 TEX. ADMIN. CODE §§ 15.141-15.148; 43 TEX. ADMIN. CODE §§ 217.121-217.124.
[111] *See* 37 TEX. ADMIN. CODE § 15.143.
[112] *See id.* § 15.146.

municipally owned utilities; (ii) identifying financial information; (iii) biometric identifiers; and (iv) crime or accident victim information.

a. Social Security Numbers held by Municipally Owned Utility

A municipally owned utility may not require an individual to disclose the individual's social security number to obtain utility services unless the municipally owned utility adopts a privacy policy that includes:

- How personal information is collected;
- How and when the personal information is used;
- How the personal information is protected;
- Who has access to the personal information; and
- The method of disposal of the personal information.[113]

The municipally owned utility must make the privacy policy available to the individual and maintain the confidentiality and security of all disclosed social security numbers pursuant to the privacy policy.[114]

A municipally owned utility that violates this requirement is liable for a civil penalty in an amount not to exceed $500 for each calendar month during which a violation occurs. The attorney general or the district attorney in the county in which the violation occurs may bring an action to recover an imposed civil penalty. Either the Attorney General or the district attorney of the county in which the violation occurs may bring an action to recover the civil penalty. In addition, the attorney general may bring an action in the name of the state to restrain or enjoin a person from violating the restriction.[115]

Other information to consider: The 87th Texas Legislature passed H.B. 872 in an effort to protect sensitive customer information from predatory practices.[116] This amendment to Chapter 182 of the Utilities Code applies to information held by a municipally owned utility that provides water, wastewater, sewer, gas, garbage, electricity, or drainage service. Effective immediately, a municipally owned utility may not disclose customer information (including the customer's address) under the Public Information Act, Chapter 552 of the Government Code, unless the customer elects to make the information public or certain exceptions apply. Also excluded from public disclosure is information: (1) that reveals whether an account is delinquent or eligible for disconnection; and (2) collected as part of an advanced metering system.

H.B. 872 essentially reverses the prior law's requirements. Before H.B. 872, utility customers had to fill out a form to request their information remain confidential. Failure to do so made the customer's information public. Now, a customer's information is protected unless the customer opts to make it public. Municipally owned utility customers may elect to make their information public

[113] TEX. BUS. & COM. CODE §§ 501.051(3), 501.052(a)(1) and (b).
[114] *Id.* § 501.052(a)(2) and (3).
[115] *Id.* § 501.053.
[116] Disclosure of Certain Utility Customer Information, 2021 Tex. Sess. Law Serv. Ch. 1025 (H.B. 872) (VERNON'S).

by filling out a form requesting disclosure of their personal information in response to Public Information Act requests.

b. Identifying Financial Information

A person, including a local government, who accepts a credit card or debit card to transact business may not print on a receipt provided to a cardholder more than the last four digits of the credit card or debit card account number or the month and year that the credit card or debit card expires.[117] A civil penalty in an amount not to exceed $500 for each calendar month during which a violation occurs. Either the Attorney General or the district attorney of the county in which the violation occurs may bring an action to recover the civil penalty. In addition, the attorney general may bring an action in the name of the state to restrain or enjoin a person from violating the restriction.[118]

c. Biometric Identifiers

A person, including a local government, may not capture a biometric identifier, defined as a retina, iris scan, fingerprint, voiceprint, or record of hand or face geometry, of an individual for a commercial purpose unless the person informs the individual before capturing the biometric identifier and receives the individual's consent to capture the biometric identifier. A person who possesses a biometric identifier of an individual that is captured for a commercial purpose may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (i) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death; (ii) the disclosure completes a financial transaction that the individual requested or authorized; (iii) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552 of the Government Code; or (iv) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant.[119] Commercial purpose is typically defined as a purpose that is intended to result in a profit or other tangible benefit.

In addition, a person who possesses an individual's biometric identifier is captured for a commercial purpose, the person must use reasonable care when storing or transmitting the biometric identifier and protect it from disclosure in a manner that, at a minimum, is as protective as the manner that the person stores, transmits, and protects any other confidential information it possesses. A person who possesses a biometric identifier of an individual that is captured for a commercial purpose must destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires unless the biometric identifier is used in connection with an instrument or document that is required by another law to be maintained for a period longer than one year, in which case the person who possesses the biometric identifier must destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law. When a biometric identifier has been collected for security purposes by an employer, the purpose for collecting the identifier is presumed to expire upon termination of the employment relationship. A person who does not comply with these

[117] *Id*. § 502.002.
[118] *Id*. §§ 1.201(27) and 502.002.
[119] *Id*. §§ 1.201(27) and 503.001.

provisions is subject to a civil penalty of $25,000 per violation in an enforcement action initiated by the attorney general.[120]

d. Crime Victim Information

A person, including a local government, who possesses crime victim or motor vehicle accident information that is obtained from a law enforcement agency may not use the information to contact, for the purpose of soliciting business, any of the following individuals: (i) a crime victim or a family member of the victim; (ii) a person, or a family member of the person, who was involved in a motor vehicle accident. A person, including a local government, who possesses crime victim or motor vehicle accident information that is obtained from a law enforcement agency may not sell information to another person for financial gain.[121]

5. Criminal Enforcement

A review of Texas laws that impose criminal liability for the unauthorized use, inspection or disclosure of information that is confidential by law has recently been addressed in a seminar paper and presentation to the Texas City Attorneys Association.[122] Of particular significance to attorneys who advise local governments is that there are in excess of 700 statutes that limit the disclosure of information or that make certain information confidential.[123] City attorneys and outside counsel who advise cities should review the statutes listed in this paper to ensure that city officers and employees are not inadvertently exposing themselves to criminal liability or civil penalties.

B. FEDERAL LAWS AND INDUSTRY STANDARDS

On the federal level, lawmakers have not implemented an omnibus data protection law. Instead, there are specific privacy laws for the types of citizen and consumer data that are deemed to be the most sensitive, such as financial, insurance and medical information; information about children and students; telephone, internet and other electronic communications; credit, consumer, and background investigation reports. Most of these federal laws apply to federal agencies and businesses, however; there are only a few federal laws that impose data protection requirements on a local government. This Section summarizes a few of the federal laws that regulate how a local government collects, discloses and maintains individually identifying information. This Section also reviews industry standards that regulate the collection of information in connection with credit card transactions.

1. Health Information Portability and Accountability Act

HIPAA establishes national standards regarding health information privacy. It applies to covered health entities and to business associates. HIPAA regulates the use, storage and disclosure of protected health information, which encompasses individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or

[120] *Id*. § 503.001(d).
[121] TEX. BUS. & COM. CODE §§ 1.201(27) and 504.002.
[122] Miles K. Risley, *The Most Dangerous Thing we do every Day is hitting "Send": Criminalized Information Transfer*, Texas City Attorneys Association Conference (2015).
[123] *Id*. at 5.

transmitted or maintained in any other form or medium. HIPAA establishes minimum protection for an individual's health information. HIPAA does not preempt a state law that imposes stricter requirements to safeguard the confidentiality, integrity and availability of protected health information.

As discussed, a local government that merely uses, stores, or exchanges medical information is likely a "covered entity" under TMRPA. A local government may also be regulated by HIPAA as a covered entity. A local government is subject to the requirements of HIPAA and must maintain the confidentiality of protected health information that it creates, transmits, uses, or maintains if it meets the definition of a covered entity as either a health plan or a health care provider.[124] A local government meets the definition of a "health plan" if it is self-insured with greater than fifty participants or if it sponsors a group health plan with greater than fifty participants and receives more than just enrollment/disenrollment and summary health information.[125] A local government meets the definition of a "health care provider" if it operates a fire department with first responders who provide emergency or ambulatory services.[126]

To comply with HIPAA, a local government must:

- Maintain the confidentiality of protected health information;
- Designate a Privacy Officer to receive complaints, coordinate compliance with respect to an individual's right to access his or her protected health information and ability to amend his or her protected health information, and issue a Notice of Privacy Practices;
- Designate a Security Officer to be responsible for ensuring that administrative, technical and physical safeguards are in place to safeguard the confidentiality, integrity, and availability of protected health information;
- Implement policies and procedures that comply with the Privacy Standards of HITECH;
- Conduct a risk assessment; and
- Implement policies and procedures that comply with the Security Standards of HITECH.[127]

The Privacy Rule requires a local government that is a HIPAA covered entity to permit individuals to access their medical records and submit a request to correct any errors in their records. The disclosure of medical information is allowed without an individual's permission for treatment, billing, and other related operations. However, all other disclosures require the written permission of the individual. A local government that is a HIPAA covered entity must also track all disclosures of protected health information and inform an individual of any use of that information. A local government that is a HIPAA covered entity must make reasonable efforts to keep communications regarding protected health information confidential.[128]

[124] 45 C.F.R. § 164.502(a).
[125] 45 C.F.R. § 160.103.
[126] *Id*.
[127] 45 C.F.R. Part 164, Subpart C and Subpart E.
[128] 45 C.F.R. § 164.522(b).

A local government that is a HIPAA covered entity performs both covered and non-covered functions. Therefore, it can minimize the scope of its coverage under HIPAA by declaring itself a "hybrid entity."[129] For a local government to establish itself as a hybrid entity, a local government should adopt a resolution that identifies those departments that create, transmit, use, or maintain protected health information and designate such departments as a health care component. Once the resolution has been adopted, only the designated departments of the local government are required to comply with HIPAA.[130]

OCR and the Texas Attorney General are authorized to enforce HIPAA. In addition to instituting an action for injunctive relief to restrain a violation under HIPAA or TMRPA, OCR and the Texas Attorney General are authorized to impose civil monetary penalties against a local government that is a HIPAA covered entity. The allowable civil penalties imposed under HIPAA are set forth below in Table 1, below.[131]

Table 1: Civil Penalties for HIPAA Violations by Covered Entity or Business Associate[132]

Culpability for Violation	Minimum per HIPAA Violation	Maximum for Identical Violation of same Provision per calendar year
Did not know and, by exercising reasonable diligence, would not have known a violation occurred	$100 per violation, with an annual maximum of $25,000 for repeat violations[133]	$50,000 per violation, with an annual maximum of $1.5 million
Violation occurred due to a reasonable cause and not willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations[134]	$50,000 per violation, with an annual maximum of $1.5 million
Violation occurred due to willful neglect – corrected in timely manner	$10,000 per violation, with an annual maximum of $250,000 for repeat violations[135]	$50,000 per violation, with an annual maximum of $1.5 million
Violation occurred due to willful neglect – not timely corrected	$50,000 per violation, with an annual maximum of $1.5 million[136]	$50,000 per violation, with an annual maximum of $1.5 million

[129] 45 C.F.R. §§ 160.103, 164.105.
[130] 45 C.F.R. § 164.105(a)(1) and (a)(2)(iii)(D).
[131] 45 C.F.R. § 160.404.
[132] HIPAA civil penalties herein are those stipulated by the HITECH Act. It should be noted that these are adjusted annually to take inflation into account.
[133] 45 C.F.R. § 160.404(b)(2)(i).
[134] 45 C.F.R. § 160.404(b)(2)(ii).
[135] 45 C.F.R. § 160.404(b)(2)(iii).
[136] 45 C.F.R. § 160.404(b)(2)(iv).

While HIPAA protects the health information of individuals, it does not create a private cause of action for an individual affected by a HIPAA violation.[137]

2. Privacy Act of 1974

The Privacy Act of 1974 regulates the federal government's collection and disclosure of personal information. For the most part, a local government entity is not subject to the Privacy Act of 1974. A local government must, however, comply with the social security number usage restrictions.[138] The social security number usage restrictions prohibit a federal, state, or local government agency from requiring an individual to provide his or her social security number to receive a right, benefit, or privilege provided by law. The restriction on collecting an individual's social security number does not apply to a required disclosure pursuant to federal law or to a system of records that existed before January 1, 1975. For instance, federal law permits a social security number to a governmental entity pursuant to a written request in connection with a civil or criminal law enforcement activity authorized by law.[139] When a government agency requests disclosure of a social security number, it must notify the individual whether the disclosure is mandatory or voluntary, what law authorizes the government agency to request the social security number, and how the social security number will be used.[140]

3. Driver's Privacy Protection Act

The DPPA restricts the release and use of personal information contained in motor vehicle records. The DPPA is codified at Chapter 123 of Title 18 of the United States Code.[141] As addressed in Part IV, A. 3., *supra*, the MVRPA adopts the provisions of the DPPA.

4. Federal Tax Information

The Internal Revenue Service ("IRS") requires a state or local government that legally receives federal tax information from either the IRS, a secondary source, or through an IRS-approved exchange agreement to protect federal tax information according to strict security guidelines.[142] Therefore, an employee of a federal, state or local agency who works with federal tax returns and tax return information must protect this information from unauthorized disclosure. An unauthorized disclosure occurs when an entity or individual with authorization to receive federal tax information discloses it to another entity or individual who does not have authority and a "need-to-know." A local government that is authorized to receive federal tax information must also establish a record of requests for the disclosure of federal tax information that it receives.[143]

5. Data Security Standard

---

[137] *Acara v. Banks*, 470 F.3d 569, 571–72 (5th Cir. 2006).
[138] 5 U.S.C. § 552a.
[139] *Id*. § 552a(b)(7).
[140] *Id*. § 552a note "Disclosure of Social Security Number."
[141] 18 U.S.C. §§ 2721 – 2725.
[142] 26 USC §§ 6103(d), (*l*)(6), (7) and (8) (2016); *see also* Internal Revenue Service, Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (2014).
[143] 26 USC § 6103(p)(4)(A).

The Data Security Standard ("DSS") is a set of comprehensive requirements to enhance payment account data security that is administered by a consortium of the major credit card companies referred to as the Payment Card Industry Security Standards Council ("PCI"). The industry standards are imposed on entities via user agreements. The DSS applies to an entity that stores, processes or transmits cardholder data. Compliance is required for *any entity* that accepts payment cards at point of service – even if it processes only one payment transaction. The extent to which a local government must comply with the DSS depends on the amount of credit card transactions that it processes. A local government that suffers a breach and is not in compliance with the DSS is subject to paying penalty fees.[144]

The DSS requires a local government that stores, processes or transmits cardholder data to build and maintain a secure network and system by installing and maintaining a firewall configuration to protect cardholder data and prohibits the use of vendor-supplied defaults for system passwords and other security parameters; protect cardholder data by protecting stored cardholder data; encrypt transmission of cardholder data across open, public networks; maintain a vulnerability management program by protecting all systems against malware and regularly update antivirus software or programs and developing and maintaining secure systems and applications; implement strong access control measures by restricting access to cardholder data by business need to know and identifying and authenticating access to system components, and restricting physical access to cardholder data; regularly monitor and test networks by tracking and monitoring all access to network resources and cardholder data; regularly test security systems and processes by maintaining an information security policy by maintaining a policy that addresses information security for all personnel.[145]

V. LITIGATION

Data privacy litigation is an evolving area of law. To establish standing, a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." With respect to data privacy litigation, the courts have typically held that a fear of future harm, alone, is insufficient to establish standing. Even where sufficient personally identifiable information has been disclosed to permit an unauthorized user to make fraudulent charges, courts generally require a plaintiff to plead actual unauthorized charges, identity theft, or fraud in order to establish an initial showing of harm.[146] Thus, the "injury-in-fact" requirement of Article III standing has been a significant barrier to plaintiffs in data breach litigation. The Supreme Court's decision in *Clapper v. Amnesty International* provides the basic test regarding whether a plaintiff meets the injury-in-fact requirement to establish Article III standing - that "threatened injury must be certainly impending to constitute injury in fact" or if there is a "substantial risk" that the harm is going to occur.[147] A handful of data-breach cases, however, have survived threshold

---

[144] Payment Card Industry, *PCI Data Security Standard Requirements and Security Assessment Procedures, v3.2*, 5 (2016).

[145] *Id.*

[146] *See, e.g., Peters v. St. Joseph Servs. Corp*., 474 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (finding alleged future harm "speculative" where disclosed information included social security numbers, addresses, medical records and bank account information, and where illicit credit card purchase was declined).

[147] *Clapper v. Amnesty International*, 133 S. Ct. 1138, 1147 (2013) (citing *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

standing challenges in the Seventh and Ninth Circuits. In these cases, the plaintiffs were able to allege injury beyond a fear of future harm.[148]

In addition to alleging harm beyond a general fear of future harm, a number of federal statutes applicable to state and local government, including the DPPA, authorize an individual to sue based on a statutory violation. The Fair Credit Reporting Act ("FCRA"), which requires a consumer reporting agency to "follow reasonable procedures to assure maximum possible accuracy" of information used for employment purposes, is one such statute. Thomas Robins sued Spokeo, a "people search engine" that relies on data aggregation, alleging violations of the FCRA due to the company publishing inaccurate personal information about him on its website. The Ninth Circuit reversed the district court's dismissal for lack of standing, concluding that Robins' alleged injury was sufficient to confer standing because violations of the plaintiff's statutory rights adequately alleged a concrete and particularized injury.[149]

In April 2015, the U.S. Supreme Court granted certiorari on the issue of whether Congress may confer Article III standing upon a plaintiff by authorizing a private right of action based on a violation of a federal law.[150] In a 6-2 opinion, the Supreme Court concluded that the Ninth Circuit failed to determine whether Robins suffered a concrete harm. The Supreme Court acknowledged that while injuries may be intangible, just because Congress grants a private cause of action does not mean an individual has established injury-in-fact. In remanding the case, the Court did not rule out the possibility that the risk of real harm can solely satisfy the concreteness requirement. Thus, a data privacy litigant must still establish a concrete harm apart from a bare procedural violation of a statute.[151]

Another data privacy case to watch are the lawsuits arising out of the massive OPM data breach. At least two class action lawsuits and over a dozen other lawsuits have been filed against the OPM over the massive breach.[152] The cases have been consolidated and transferred to the U.S. District Court for the District of Columbia. The American Federation of Government Employees and the National Treasury Employees Union allege that the OPM and its contractors violated the 1974 Privacy Act, the Federal Information Security Management Act, the Federal Information Security Modernization Act, the Administrative Procedure Act, the Fair Credit Reporting Act, and that OPM's and its contractor's actions and inactions constituted negligence, negligent misrepresentation and concealment, invasion of privacy, and breach of contract by neglecting to secure employees' personal data, which resulted in financial and emotional harm. More specifically, the petition seeking damages stated that "OPM violated our constitutional right to informational privacy by recklessly disregarding its Inspector General's warnings over many

---

[148] *In re Adobe Systems, Inc. Privacy Litig*., 2014 WL 4379916 (N.D. Cal. 2014) (finding that plaintiffs sufficiently alleged concrete injury where hackers specifically targeted personally identifiable information after an intrusion, used Adobe's own decryption keys and posted personally identifiable information on the Internet); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig*. (Sony II), 996 F. Supp. 2d 942, 962 (S.D. Cal. Jan 21, 2014) (concluding that plaintiffs successfully alleged injury-in-fact where their personal information was collected by Sony and was subsequently wrongfully disclosed due to an unauthorized intrusion); *Corona v. Sony Pictures Entm't Inc*., 2015 WL 3916744 (C.D. Cal. 2015) (alleged theft and publication of personally identifiable information on online file-sharing website is sufficient to establish Article III standing).

[149] *Robins v. Spokeo, Inc*., 742 F.3d 409 (9th Cir. 2014).

[150] *Spokeo, Inc. v. Robins*, 135 S. Ct. 1892 (2015).

[151] *Id*.

[152] Plaintiff's Consolidated Amended Complaint, *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig*., 266 F. Supp. 3d 1 (D.D.C. 2017), aff'd in part, rev'd in part and remanded, 928 F.3d 42 (D.C. Cir. 2019).

years about its IT security deficiencies."[153] The litigants seek, in part, that the federal government provide the affected individuals with lifetime credit monitoring services, fraud protection, and identity theft insurance.[154] The lawsuit was thrown out in 2017 when the federal district court ruled that the Privacy Act, the law that the suit was based on, used the word "disclosed" in relationship to data and ruled that the law did not apply in cases where data was stolen but not publicly revealed.[155] However, the U.S. Court of Appeals for the D.C. Circuit largely sided with the two federal employee unions in their lawsuit against the OPM and the federal contractor. The appellate court ruled that federal employees do indeed have standing to sue the government over its failure to protect personally identifiable information that led to the massive data breaches in 2015, reversing the decision of the lower court.[156]

VI. CONCLUSION

A city is obligated to ensure the privacy, security and integrity of data it collects. Public entities hold massive amounts of personal and business data, making them a target for criminals seeking financial gain, cyber espionage, or hacktivism. Yet, the cybersecurity efforts of public entities rank below that of other major industries. Regardless of whether the goal of the cybercriminal is monetary or to gather intel, a breach can inflict a great deal of harm on individuals, businesses, and the public sector. Due to the numerous state and federal laws that regulate data privacy, a public entity must comply with industry regulations, laws that regulate financial and medical activities, laws that regulate the type of data collected, and laws that restrict the disclosure of information based on the status of the individual. In addition, a public entity must comply with various regulations imposed on the state and federal levels, as well as by state agencies and industries via user agreements. The "injury-in-fact" requirement of Article III standing is a significant barrier to plaintiffs seeking recovery as a result of a data breach.

As data privacy litigation develops, however, the barrier to establishing injury may prove to be less elusive. City attorneys and outside counsel who advise cities regarding how to comply with the multitude of laws that regulate the collection, storage, release, availability, integrity, or destruction of individually identifying information should evaluate the potential liability of cities in the event of a breach or unauthorized disclosure or due to the failure to comply with notification requirements, mitigate harm, or implement privacy and security policies and procedures. While there are a number of federal and state laws that impose data privacy requirements on cities, city attorneys and outside counsel should advise clients to initially focus any efforts to ensure compliance on the laws and regulations that have the potential to impose the greatest liability. Admittedly, this is a moving target that shifts on the sands of the readiness of a city's information technology infrastructure and employees, the state of data privacy litigation, and whether lawmakers authorize individuals to seek remedy against public entities. Based on personal experience, however, a city that violates a data privacy or security requirement can minimize - and even avoid - civil penalties if it demonstrates that it is in the process of making a good faith effort to comply with data privacy requirements.

---

[153] *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1 (D.D.C. 2017), aff'd in part, rev'd in part and remanded, 928 F.3d 42 (D.C. Cir. 2019).

[154] *Id.*

[155] *Id.*

[156] *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 51 (D.C. Cir. 2019).

APPENDIX A

SUMMARY OF THE IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT AND RELATED STATUTES

State Statutes: Tex. Bus. & Com. Code § 521.002, 521.052 and 521.053; Tex. Loc. Gov't Code § 205.010(b); Tex. Gov't Code § 2054.1125(b).	
Sensitive Personal Information Definition	The statute applies to "Sensitive Personal Information", which includes an individual's first name or first initial and last name in combination with any one or more of the following, if the information is not encrypted: • Social Security number; • Driver's license number or government-issued identification number; and • Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's account. In addition, SPI is information that identifies an individual and relates to: • The physical or mental health or condition of the individual; • The provision of health care to the individual; or • Payment for the provision of health care to the individual.
Persons Covered	A business, local government or state agency that conducts business in Texas and owns, licenses or maintains computerized data that includes sensitive personal information.
Standard for Triggering	The statute is triggered upon discovery or the receipt of notification of a breach of system security. "Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key to decrypt the data.
Specific Notice Content Requirements	Not specified in statute.
Time to Notify Affected Persons of Breach	Disclosure should be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of law enforcement agency that determines that the notification will impede a criminal investigation. Any person who maintains computerized data that includes sensitive personal information not owned by the person must notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Exemptions	Sensitive personal information only includes data items that are not encrypted unless the encryption key is also breached.

Penalty	The Attorney General may bring a civil suit for damages or an injunction. A person who violates the statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. A person who fails to take reasonable action to comply with notification requirements is liable to the state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day the person fails to take reasonable action to notify with a maximum penalty of $250,000 for a single breach. If it appears to the Attorney General that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the Attorney General may bring an action in the name of the State against the person for a temporary restraining order or by a permanent or temporary injunction. These provisions do apply to a local government.
Private Right of Action	A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.
Other Provisions	Affected individuals residing in states with data breach notification statutes must be notified in accordance with their state's law. If an entity must notify over 10,000 individuals of a breach, the entity must notify each consumer reporting agency of the timing, distribution, and content of the notices without unreasonable delay. A business must implement and maintain reasonable procedures, including appropriate corrective action, to protect from unlawful use or disclosure of sensitive personal information, such as shredding, erasing, or other similar means of modifying sensitive personal information to make it unreadable or indecipherable. This provision does not apply to a local government. Notification must be sent to the attorney general regarding a breach of system security under Business and Commerce Code Sec. 521.053 to include the number of affected residents that had been sent a disclosure of the breach by mail or other direct method of communication at the time of notification. The attorney general would have to then post on the attorney general's website a comprehensive listing of all received notifications of security system breaches, and the listing would have to be updated within 30 days after notification of a new breach of system security was received. Sensitive personal information and other confidential information that had been reported to the attorney general under Sec. 521.053 would be excluded from the listing.

APPENDIX B

SUMMARY OF THE TEXAS MEDICAL RECORDS PRIVACY ACT AND RELATED STATE LAWS, FEDERAL LAWS, AND REGULATIONS

State and Federal Statutes and Regulations: Tex. Health & Safety Code, Chapter 181; Tex. Loc. Gov't Code § 205.010(b); Tex. Bus. & Com. Code § 521.002 and 521.053.	
Protected Health Information Definition	Protected health information ("PHI") is not defined in the Texas Medical Records Privacy Act (the "TMRPA") but TMRPA incorporates the definition of PHI under the Health Insurance Portability and Affordability Act ("HIPAA") and the Privacy Standards. Thus, for purposes of TMRPA, PHI means: • Individually identifiable health information transmitted or maintained in any form or medium by a covered entity or its business associate; or • Health information (including demographic information) that relates to an individual's physical health, mental health, the provision of health care, or health care payment that identifies the individual. PHI does not include: (i) Family Educational Rights and Privacy Act (FERPA) or (ii) Employment records unless the records are electronically transferred. For a local government, "Sensitive personal information" has the meaning assigned by the ITEPA. In addition, the breach of PHI by a covered entity that is a governmental unit triggers the notice requirements under the ITEPA. Individually Identifiable Health Information means information that is collected from an individual, including demographic information that either identifies the individual or can be used to identify the individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to either: • The past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or • The past, present, or future payment for the provision of health care to an individual.
Persons Covered	TMRPA applies to a "Covered Entity", which is defined as any person who for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis: (i) engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI; (ii) comes into possession of PHI; (iii) obtains or stores PHI under TMRPA; or (iv) is an employee, agent, or contractor of a covered entity insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits PHI. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or a person who maintains an Internet site.

Standard for Triggering	TMRPA does not include any breach notification requirements. A local government that is a TMRPA covered entity and experiences a breach incident must comply with breach notification requirements if the entity owns, licenses, or maintains computerized data that includes SPI and the breach compromises the security, confidentiality, or integrity of the information. Under the ITEPA, "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of SPI maintained by a local government, including data that is encrypted if the person who acquires the data has the key to decrypt the data. Such a breach triggers the notice requirements under the ITEPA. The ITEPA is triggered upon discovery or the receipt of notification of a breach of system security.
Specific Notice Content Requirements	Not specified in statute.
Time to Notify Affected Persons of Breach	TMRPA incorporates HIPAA's definition of PHI. The definition of SPI under TMRPA is very similar to the definition of PHI under HIPAA. Therefore, the breach of PHI by a TMRPA covered entity triggers the notice requirements under the ITEPA. Thus, disclosure to the affected persons(s) should be made as quickly as possible or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. However, disclosure may be delayed at the request of a law enforcement agency if the agency determines that the notification will impede a criminal investigation.
Exemptions	Partial Exemption for Records of Employer: Except for regulations regarding the re-identification of PHI, marketing of PHI, sale of PHI, and the electronic disclosure of PHI, TMRPA does not apply to PHI held by an employer. Workers' Compensation: TMRPA does not apply to workers' compensation insurance, a function authorized by Title 5 of the Labor Code, or any person in connection with providing, administering, supporting, or coordinating any of the benefits under a workers' compensation self-insured program. Employee Benefit Plans: TMRPA does not apply to an employee benefit plan, a covered entity or person acting in connection with an employee benefit plan. Offenders with Mental Impairments: TMRPA does not apply to an agency listed or described in Health and Safety Code, Section 614.017 that disclosures, receives, transfers, or exchanges the PHI relating to a special needs offender or a juvenile with a mental impairment in the custody of the agency for purposes of continuity of care and services. Among other entities, listed agencies include local jails regulated by the Commission on Jail Standards, a municipal or county health department, a hospital district and a judge with jurisdiction over juvenile or criminal cases. Crime Victim Compensation: TMRPA does not apply to an entity in

	connection with providing, administering, supporting, or coordinating benefits regarding compensation to crime victims as provided by Code of Criminal Procedure, Chapter 56, Subchapter B.
Penalty	The Attorney General may institute an action for civil penalties for violations of TMRPA not to exceed: • $5,000 per violation per year committed negligently, • $25,000 per violation per year if committed knowingly or intentionally, or • $250,000 per violation if the covered entity knowingly or intentionally used the PHI for financial gain. Penalty Reduction: The total amount of a penalty assessed against a covered entity under TMRPA in relation to a violation of the electronic disclosure of PHI is capped at $250,000 annually if the court finds that the disclosure was made to another covered entity for treatment, payment, health care operations, performing an insurance or health maintenance organization function or as otherwise authorized or required by state or federal law and the court finds that: • The PHI disclosed was encrypted or transmitted using encryption technology designed to protect against improper disclosure; • The recipient of the PHI did not use or release the PHI; or • At the time of the disclosure of the PHI, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of PHI. Mitigation: In a proceeding to impose an administrative or civil penalty due to the disclosure of individually identifiable health information, a covered entity may introduce, as mitigating evidence, evidence of the entity's good faith efforts to comply with: • State law related to the privacy of individually identifiable health information; or • HIPAA and Privacy Standards. In determining a penalty imposed on a covered entity that is licensed by a state agency, a court or state agency must consider these factors: • The seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure; • The covered entity's compliance history; • Whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose PHI is involved in the violation; • Whether the covered entity was certified at the time of the violation under Health & Safety Code, Section 182.108; • The amount necessary to deter a future violation; and • The covered entity's efforts to correct the violation.
Private Right of Action	A violation of this statute is also a deceptive trade practice under the Texas Deceptive Trade Practices Act; however, the Texas Deceptive Trade Practices Act does not apply to a local government.

Other Provisions	Electronic Disclosure of PHI: A covered entity may not electronically disclose an individual's PHI without a separate authorization from the individual or the individual's legally authorized representative for each disclosure. The authorization is not required if the disclosure is authorized or required by state or federal law. A covered entity may provide general notice by: • Posting a written notice in the covered entity's place of business; • Posting a notice on the covered entity's Internet website; or • Posting a notice in any other place where individuals whose PHI is subject to electronic disclosure are likely to see the notice. Training: Each covered entity must train its employees on state and federal laws regarding PHI within 90 days after the employee is hired and within one year of a material change in law concerning PHI. Each employee must sign a statement verifying the employee's training. The covered entity must maintain these signed statements for six years. Sale of PHI: A covered entity may not disclose an individual's PHI to anyone in exchange for direct or indirect remuneration. Marketing Using PHI: PHI may not be used or disclosed for marketing purposes without first obtaining consent or authorization from the individual. Written communications must explain the recipient's right to removal from the mailing list, and removal must be accomplished within 45 days after the receipt of the request. Re-identification of PHI: A covered entity may not re-identify or attempt to re-identify PHI to identify an individual unless the individual provides prior consent or authorization. The Privacy Standards: TMRPA adopts the Privacy related to an individual's right to access to his/her PHI and ability to amend his/her PHI.

APPENDIX C

CYBERSECURITY TERMINOLOGY

Advanced Persistent Threat (APT) – Targeted attacks differ from APTs in the same way a handgun differs from a state-of-the-art military issued rifle: sophistication, engineering, and user. APTs are attacks that use code and tools that have been designed from the group up by groups of well-talented salaried engineers. APTs are also state-sponsored attacks—which means that actual governments are behind them, rather than just a small group of hackers as is in the case of targeted attacks. APTs are much more serious in scope and firepower than targeted attacks, and typically only go after big targets like government agencies.

Alert – A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.

Attack – an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Attack signature – A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities.

Attribution – the process of tracking, identifying, and laying blame on the perpetrator of a cyberattack or other hacking exploit.

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization -– Access privileges granted to a user, program, or process or the act of granting those privileges.

Backdoor – An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

Brute Force Attack – A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.

Call back – Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact.

Compromise – Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Continuous Monitoring – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Controlled Unclassified Information – Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

CONUS – CONUS refers to the continental United States. To state that delivery is CONUS is to say that a procurement delivery could be anywhere in the continental U.S, excluding Hawaii and Alaska.

Cybercrime operation – the biggest difference between a targeted attack and a cybercrime operation is the scope. A cybercrime operation aims to victimize as many users as possible in the shortest amount of time to outrace security efforts, while a targeted attack has a narrow scope. Targeted attacks are deliberate, purposeful, and persistent while cybercrime operations are usually automated, opportunistic, or indiscriminate in nature. Cybercrime operations are also mostly driven by financial intentions, while targeted attacks have the primary goal of stealing information.

Cybersecurity Event – Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Cybersecurity Incident – An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Cybersecurity Threat – See *threat.*

Data breach – a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Data leak/Inadvertent disclosure – Type of incident involving accidental exposure of information to an individual not authorized access.

Data Loss Prevention (DLP) – DLP software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized parties by either malicious intent or an inadvertent mistake. Sensitive data includes private or company information, intellectual property (IP), financial or patient information, credit-card data and other information (Wikipedia)

Demilitarized Zone (DMZ) - In network security, a network that is isolated from, and serves as a neutral zone between, a trusted network (for example, a private intranet) and an untrusted network (for example, the Internet). One or more secure gateways usually control access to the DMZ from the trusted or the untrusted network

Digital Forensics – The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

DoS/DDoS – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). DDoS is a denial-of-service technique that uses numerous hosts to perform the attack.

Encryption – Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Exploit – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Exposure – A system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

Firewall – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

Hacktivism – or activism-related hacking attacks are different from targeted attacks due to the former's one-off, vandalistic nature. They are often more like nuisances—not that harmful, and something that can be dealt with easily, like the defacement of a public wall. Hacktivism attacks often yield no network penetration and little to no information theft of any soft. They are also done with the maximum amount of visibility—they are designed to be seen, rather than staying out of sight like targeted attacks are designed to do.

Hardening - the process of securing a system by reducing its surface of vulnerability.

Host Intrusion Detection System (HIDS) - A host-based intrusion detection system is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system operates.

Host Intrusion Prevention System (HIPS) - HIPS is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. In other words, a Host Intrusion Prevention System aims to stop malware by monitoring the behavior of code. This makes it possible to help keep your system secure without depending on a specific threat to be added to a detection update.

Indicator – A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.

Information Sharing and Analysis Organization (ISAO) – Any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability.

Intrusion Detection System (IDS) - Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS, which become part of your network to detect and stop potential incidents.

Intrusion Prevention System (IPS) - Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS, which become part of your network to detect and stop potential incidents.

IP Reputation Block – the process of correlating source IP addresses against databases of known malicious IP addresses, and stopping them before they have a chance to make it into a network.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Multi-factor Authentication (MFA) – Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Network Access Control (NAC) - a computer networking solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network

Network Forensics Tool (NFT) -Network Forensics tools provide the ability to store, analyze and display all network data to reconstitute an even so an investigator can determine what happened on the network.

Observation – An event (benign or malicious) on a network or system.

Passive attack – An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping). An attack that does not alter systems or data.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration testing – Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Personal identifying information – means information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code.

Phishing – A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Plaintext/Cleartext – Intelligible data that has meaning and can be understood without the application of decryption. Unencrypted information.

Port – A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Port scanning – Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Reconnaissance/information gathering – the process of collecting information about an intended target of a malicious hack by probing the target system.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State/Nation.

Role-based access control – Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Scanning – Sending packets or requests to another system to gain information to be used in a potential subsequent attack.

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Segmentation - Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

Sensor – An intrusion detection and prevention system component that monitors and analyzes network activity and may also perform prevention actions.

Sensitive personal information – means (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of

the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

Sniffing – A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

Social engineering – A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. 2. The deliberate inducement of a user or resource to take incorrect action.

Tactics, Techniques, and Procedures (TTPs) – The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Targeted attack – An attack that fulfills three main criteria: 1.) the attackers have a specific target in mind and has been shown to have spent considerable time, resources, and effort in setting up or carrying out the targeted attack. 2.) the main aim of the targeted attack is to infiltrate the target's network and steal information from their servers or significantly impact the availability, integrity, confidentiality, or non-repudiation of the affected information systems. 3.) the attack is persistent, with attackers expending considerable effort to ensure the attack continues beyond the initial network penetration and exfiltration of data. Targeted attacks are often discovered years after the fact.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Actor – An individual or a group posing a threat.

Threat Information – Any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.

Threat Intelligence – Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Threat Intelligence Report – A prose document that describes TTPs, actors, types of systems and information being targeted, and other threat-related information.

Threat Shifting – The response of actors to perceived safeguards and/or countermeasures (i.e., security controls), in which actors change some characteristic of their intent/targeting in order to avoid and/or overcome those safeguards/countermeasures.

Tool Configuration – A recommendation for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information

TOR – is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays[to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Virtual Local Area Network (VLAN) - a logical subnetwork that can group together a collection of devices from different physical LANs. Larger business computer networks often set up VLANs to re-partition their network for improved traffic management.

Virtual Private Network (VPN) - a method employing encryption to provide secure access to a remote computer over the Internet.

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Watering Hole Attack – A security exploit where the attacker infects websites that are frequently visited by members of the group being attacked, with a goal of infecting a computer used by one of the targeted group when they visit the infected website.

Zero-day – A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability. Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.

SOURCES

National Institute for Standards and Technology Special Publication definitions:
https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

Texas Administrative Code RULE §202.1:
http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=1

Chapter 521, Texas Business and Commerce Code:
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm

Understanding a Targeted Attack: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack

APPENDIX D

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

AN INTRODUCTORY GUIDE

Cyber incidents and data breaches continue to proliferate globally, targeting organizations across all industries and sectors. The worldwide monetary loss to cybercrime is measured in the hundreds of billions. The global cyber threat is a challenge due to the nature of transnational commerce, its interconnected networks and supply chains, and the use of electronic payment systems. This is compounded by the proliferation of increasingly sophisticated tools available to cybercriminals, jurisdictional uncertainty in transnational cases, and lenient attitudes towards cybercrime in some countries. Cybercrime has no borders and no border protection. In 2018, transnational cybercrime investigation cases led by the U.S. Secret Service accounted for $1.9 billion in actual financial losses and $6.8 billion in potential losses averted due to law enforcement action.

A comprehensive and integrated approach to cybersecurity with organized cyber incident response policies is the only sustainable path to achieving continuity in uncertain times. An organization cannot anticipate every disruption or prevent every cyber incident. Even the most advanced tools and methods do not guarantee perfect cybersecurity implementation. Organizations must anticipate an evolving risk environment and be prepared to respond at a moment's notice when a disruption to their business occurs. Accomplishing continuity of operations requires a resilient approach to cybersecurity - an integrated, holistic way to manage security risks, business continuity, disaster recovery, and information technology (IT) operations. To achieve this, a comprehensive plan for incident management and incident response (IR), with regular testing and updating, is crucial.

Criminals maneuver in the anonymity of cyberspace using tradecraft to limit risk from law enforcement. To build on the principle of deterrence, the role of law enforcement in an organization's IR plan is critical to our nation's cybersecurity strategy. It is essential for an organization to develop a trusted relationship with law enforcement and integrate them into the development of a cyber IR plan. This early preparation can facilitate a mutually created framework for restoring business operations to a victim organization while assisting in evidence collection for law enforcement. Preplanning and rehearsing a cyber IR plan helps target the relevant sources of evidence for a criminal investigation, while facilitating speedy restoration of business operations. Engagement with law enforcement before, during, and after a cyber incident will increase opportunities to arrest and prosecute cybercriminals. This collective effort will result in the enhancement of our strategic focus to dissuade criminals from continuing to target your organization. A growth in partnerships between the private sector and law enforcement built on trust and communication will continue to shape cyber resiliency, layer by layer.

The U.S. Secret Service has extensive experience in cyber IR and the subsequent criminal investigations, and we offer this guide outlining basic steps an organization can take before, during, and after a cyber incident. This guide is built upon an in-depth analysis of the methods and tools used to identify, locate and arrest significant cybercriminals, the industry technical framework of the National Institute of Standards and Technology (NIST), and the legal framework of the Department of Justice.

Figure 1: NIST Framework

In 2014, NIST published a Framework for Improving Critical Infrastructure Cybersecurity (Figure 1), with revisions in 2017 and 2018.

In 2015, the Department of Justice published Best Practices for Victim Response and Reporting of Cyber Incidents, with a revision in 2018.

The four sections of this guide (Understand, Prepare, Execute, and Debrief) describe what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations. This guide does not constitute legal advice and is only for reference purposes. The corresponding flowchart (Figure 2) reflects these sections and provides an at-a-glance view of the basic steps described below. The sequence of these steps is not fixed, and will depend on your organization's specific needs.

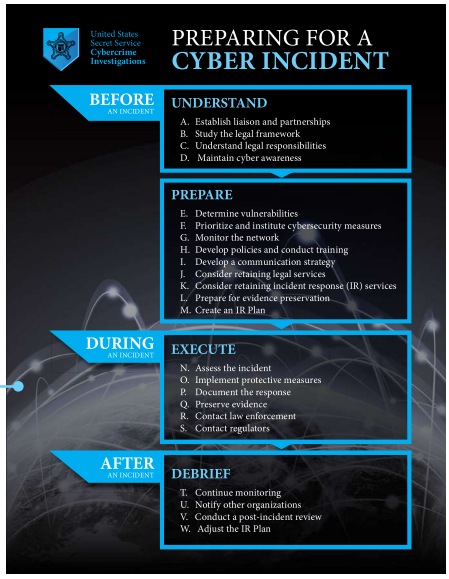


Figure 2: U.S. Secret Service Cyber Preparedness Chart

UNDERSTAND

A. Establish liaison and partnerships:

Begin by identifying law enforcement agencies responsible for combating cybercrime within your geographic area. Determine what cybersecurity information and resources they have available publically or through partnership initiatives.

The Secret Service operates **Cyber Fraud Task Forces (CFTFs)**. This is a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia. The goals and priorities of the CFTFs are to combat cybercrime through prevention, detection, mitigation, and investigation of cyber incidents. The 40 strategically located CFTFs boast a strong alliance of over 4,000 private sector partners, 2,500 international, federal, state and local law enforcement partners, and 350 academic partners. State and local law enforcement CFTF partners are trained by the Secret Service National Computer Forensics Institute (NCFI). The CFTFs host partner meetings to discuss the latest in prevention, detection, mitigation, and cooperation among law enforcement and private sector organizations. CFTF partners receive quarterly bulletins, which include current trends in cybercrime and detection, policy, legal topics, and other CFTF developments. This partnership model facilitates incident response and allows the Secret Service to be a trusted resource to an organization for guidance during an initial stage of a cyber-incident.

The U.S. Secret Service shares the law enforcement responsibility for protecting the United States from cybercriminals with the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) Homeland Security Investigations (HSI) and Cybersecurity and Infrastructure Security Agency (CISA). Although there is overlapping jurisdiction in some authorities, the FBI has sole jurisdiction on cybercrime related to counter terrorism, foreign intelligence and nation state adversaries. Additionally, local and state police departments may have resources dedicated to investigate cybercrime or maintain a relationship with a federal task force.

When and where possible, you are encouraged to establish liaison with public and private cybersecurity organizations. The cyber domain evolves continually and information sharing is crucial to remain current on cybercrime trends, tactics, and methods.

B. Study the legal framework:

Consult with external and internal legal experts who are familiar with technology, data breaches, and cyber incident management. Learn the laws and regulations governing communications, data privacy, information-sharing, and monitoring. Learn where your organization is storing the data and where the individuals/ entities, whose data your organization is storing, reside, to determine jurisdiction over the data. In 1986, the United States Congress enacted the Computer Fraud and Abuse Act (CFAA), as an amendment to **18 U.S.C. 1030**. The CFAA has since been amended multiple times to address advancements in technology and cybercrime. The CFAA criminalizes knowingly accessing a computer without authorization, obtaining protected information, with the intent to defraud, intentionally causing unauthorized damage to a protected computer, knowingly and with intent to defraud trafficking in passwords or access information, and extortion involving computers.

Multinational organizations, particularly those transmitting and storing data transnationally, must make additional considerations when working towards greater cyber resilience. These considerations will vary based on the specific country where an organization operates, transmits and stores data. Consider the citizenship of those whose data your organization handles. Learn if and how your organization is protected by laws and regulations as a potential victim of a data breach. For example, the European Union (EU) has enacted a single EU-wide data protection reform, the General Data Protection Regulation (GDPR), allowing EU citizens to better control their personal data, while allowing businesses to reduce red tape and to benefit from greater consumer trust.

C. Understand legal responsibilities:

Understand your organization's responsibility regarding data protection and data breach reporting under federal, state, local, and international law. Determine the threshold for mandatory breach reporting and which entities require notification as there is no comprehensive law in the United States that addresses data privacy and protection, but there are sector-specific laws. The **U.S. Federal Trade Commission (FTC)** is responsible for protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices, whereas the **U.S. Securities and Exchange Commission (SEC)** was established to protect investors, maintain fair, orderly, and efficient markets. The **U.S. Department of Health and Human Services (HHS)** oversees the compliance with the **Health Insurance Portability and Accountability Act (HIPAA)**. Additionally, each state may have its own legislation concerning data privacy.
Determine if your organization is required to implement threat detection and data loss prevention programs for compliance under federal, state, local, and international law. Identify the legal consequences of decisions your organization will make, during a potential incident, and how to prepare for potential interaction
with law enforcement and/or regulatory agencies. If using contracted third-party services for storing or transmitting your organization's data, determine how responsibility is shared between your organization and contracted third-party service providers. Determine what provisions to include in contracts and agreements with these providers, to include including cooperation during a cyber incident, and furnishing information to IR firms and law enforcement agencies. Consider cyber insurance, if available and suitable for your organization.

D. Maintain cyber awareness:

Continually learn about existing and emerging cyber threats and risk management strategies by participating in cybersecurity events and educational programs. Such events are often sponsored by private firms as well as law enforcement agencies. Develop a further understanding of the threat environment and the protective measures available to your organization. Subscribe to receive timely information about cyber security issues, vulnerabilities, and exploits from reputable cybersecurity organizations. For example, DHS created the **National Cyber Awareness System** which provides subscribers access to timely information about security topics and threats. For a more customized approach to preparedness for your organization, consider seeking industry-specific guidance and consult with cybersecurity
services organizations.

PREPARE

E. Determine vulnerabilities:

Identify network and device vulnerabilities specific to your organization's operations. It is important to consider all devices, stationary and mobile, with network and data access. Such devices include desktop and laptop computers, printers, copiers, internet of things (IoT) devices, cellphones (organization and employee-owned), and any other devices that are connected to a network or other devices, wirelessly or through Ethernet cables. Assess how and where your organization backs up data. Evaluate vulnerabilities associated with using contracted third-party service providers and other outside entities that host and/or have access to your organization's network and data. These include cloud and backup storage, software services, or any other contractors and vendors that have some level of access to your network and data. Learn how your organization's data is being protected by these contracted third-parties, and understand your responsibilities and liabilities when it comes to using contracted third-parties. When entering into a contract with a third-party vendor, ensure your contract includes a stipulation on them notifying your organization when they are subject of a data breach, and on what effect the breach has on your network and data.

The Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. If your organization's line of work can potentially affect critical infrastructure and public safety, the directive delivers policy statements defining the roles various federal, state, and local agencies will play in carrying out in the protection of critical infrastructure. In 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 established DHS CISA, a federal risk advisor, collaborating with partners to defend against threats and build a more secure and resilient infrastructure.

F. Prioritize and institute cybersecurity measures:

Ensure that basic cybersecurity best practices, such as robust passwords, multi-factor authentication, disabling USB storage devices, and perimeter defense (firewalls) are instituted. As an additional layer of security, consider using data encryption that resides on networks and devices (at rest), as well as for data that is transmitted (point-to-point). Subsequently determine which data, assets, and services warrant the greatest protection and prioritize cybersecurity efforts based on mission-critical needs. Specific measures may include, instituting access controls and network segmentation that appropriately limit the availability of data, particularly mission-critical data, and maintaining server logs (firewall, event and active directory), which could be critical to establishing the cause and origin of a cyber incident. Consider procuring cybersecurity technology and services that align with threats that would cause most harm to your organization, and may include intrusion detection capabilities, data loss prevention, and traffic filtering or scrubbing. Test technological solutions regularly, to include involving contracted third-party service providers, to ensure they perform as expected. Routinely review access privileges and discontinue access when employees leave your organization. Routinely back up data, ensure the backups are not connected to the network, and are stored securely offsite.

G. Monitor the network:

Consider monitoring your organization's network traffic (internal and external, inbound and outbound), which can be critical to detecting, analyzing, preventing, and addressing cyber incidents. However, prior to procuring technology to monitor systems and devices for cybersecurity threats, understand your organization's responsibilities under federal, state, local, and international law and ensure compliance when conducting such monitoring. Consider using log-in banners, user agreements, workplace policies, training, and written acknowledgement from employees and contractors to inform that their use of the network constitutes consent to your organization monitoring the communications, in accordance with applicable laws and regulations. The **Cybersecurity Information Sharing Act of 2015 (CISA)**, explicitly authorized organizations to monitor their own information systems, and, upon written consent, the systems of other organizations, for cybersecurity purposes. The Department of Homeland Security (DHS) created the **Automated Indicator Sharing (AIS)** to enable the exchange of cyber threat indicators between the Federal Government and the private sector. Note that the laws in some countries and regions may restrict your ability to monitor the content of employees' communications and may not allow employees to consent to such monitoring. Consider additional steps to preventing employee error, such as implementing email filtering and web restrictions.

H. Develop policies and conduct training:

Develop internal policies addressing cybersecurity in general, and, more specifically, for handling cyber incidents. Develop a framework for your organization's employees to be cognizant of and maintain good "cyber hygiene," and encourage employees to recognize and swiftly report suspicious activity. Studies have shown that employees have continually been a weak link in organizations' cyber resilience, intentionally (insider threat) or unintentionally (insider risk). Conduct regular briefings with employees and keep them informed on cybersecurity procedures and responsibilities. If possible, test your employees to enhance cybersecurity awareness.

I. Develop a communication strategy:

After having acquired an understanding of the legal framework and specific reporting requirements, develop a communication strategy for your organization to implement during a cyber incident. Establishing a communication strategy prior to a cyber incident, which requires a swift response, should be an important component of an organization's preparation phase. Consider establishing "out of band" communication methods. Determine how you will communicate with all employees, those that will participate in the IR Plan execution and those who will not. At a minimum, an organization should have preapproved notification templates for law enforcement, regulatory agencies, and, if applicable, media. Communication templates can vary depending on a specific situation and reporting requirements. Continuous proactive liaison with law enforcement will help understand the requirements law enforcement may have during an incident and a subsequent investigation, and should be included in your organization's communication strategy.

J. Consider retaining legal services:

Consider retaining the services of experts to address legal issues and assist with decision making during a potential cyber incident. Include them in IR planning and tabletop exercises for an opportunity to address questions regarding interacting with contracted third-parties, issuing public communications, addressing local reporting requirements, coordinating with law enforcement, and engaging with IR firms.

K. Consider retaining IR services:

Consider retaining an IR firm to expedite your organization's response to a cyber incident. If considering an IR firm, ensure that it has experience with local data protection laws and regulations, is using forensically sound methods of evidence collection and data preservation, and has well established channels of communication with law enforcement. Law enforcement is responsible for investigating criminal violations with the objective of identifying, apprehending, and prosecuting perpetrators. Thus, law enforcement is focused on collecting information about the criminal conduct, and is frequently limited to technical data that can be used to track activities and events on the network. This technical information may be distinct from, but sometimes commingled with information collected by the IR firm, and law enforcement may need to coordinate with the IR firm to obtain technical data the firm has already collected. This coordination can minimize disruption of an organization's operations, avoid duplication of efforts, and expedite an investigation.

L. Prepare for evidence preservation:

While prioritizing and instituting preventative cybersecurity measures is of utmost importance, preparation should include preemptive measures for dealing with an incident when, not if, one occurs. This includes understanding that evidence preservation begins well before having detected a cyber incident. Some evidence preservation will depend on the type of incident and organization-specific vulnerabilities, but there are general rules to ensuring evidence preservation. The average cyber incident remains undetected for months. There are rules your organization should implement to support evidence preservation during an incident, such as maintaining server logs (firewall, event and active directory) for at least a year and maintaining a current network map. Maintaining an up-to-date network map, that includes authorized remote connections, will expedite detection and isolation of an incident, as well as assist with the investigation and prosecution.

M. Create an Incident Response (IR) Plan:

Develop an IR Plan with specific and concrete procedures to follow in the event of a cyber incident. The IR Plan should include the following:

a. **An IR Team consisting of decision makers and critical personnel (senior management, legal counsel, human resources, corporate security, IT security, public relations), and, if needed, a retained IR firm. If retaining the services of an IR firm, collaborate with the IR firm on your organization's IR Plan and review their processes.**

b. **Assignment of specific tasks and timelines for the completion of critical tasks.**

c. **Contact information for the members of the IR Team, day and night, and how to proceed if they are unreachable or unavailable.**

d. **Contact information for senior management, communications personnel, shareholders, and legal counsel, and a description of the circumstances under which each should be contacted.**

e. **Consider "out of band" communication methods to coordinate during an IR event, so that when a cyber incident occurs, you are not using your organization's integrated communications (email, phones, etc.) to prevent intruders from monitoring your organization's IR.**

f. **Prioritization of what mission-critical data, networks, assets, or services should receive primary attention during an incident and procedures for implementing security measures, such as segmenting the network (isolating the threat).**

g. **Procedures for preserving evidence for potential criminal prosecution. These should include procedures already in action (server logs and network maps), along with predetermined incident-specific procedures that can be quickly implemented as part of the IR Plan.**

h. **Instructions for contacting and engaging with law enforcement, to include providing known, and relevant information about the incident.**

i. **Steps for resolving legal questions, such as compliance with data protection under the law.**

j. **Procedures for notifying regulatory agencies, if and when applicable.**

k. **Instructions for contacting contracted third-party service providers, and other outside entities who host the affected data and services, such as cloud storage service providers and commercial data centers.**

l. **Procedures for restoring backed-up data, including measures for insuring the integrity of backed-up data before restoration.**

m. **Templates for issuing public communications for compliance with under the law.**

n. **Conduct tabletop exercises to ensure that employees become and remain familiar with the IR Plan, and that communication channels and emergency processes remain up-to-date.**

o. **If using contracted third-parties to transmit and store data, inquire about and study their IR Plan.**

p. **Keep the IR Plan up-to-date and maintain hard copies easily accessible by the IR Team. Do not save the digital copy of the IR Plan on your primary systems where it can be accessed by intruders.**

Following the above steps will save valuable time during an incident. Documenting the steps taken will save valuable time during your organization's interaction with law enforcement and will create a solid foundation for investigating and prosecuting the intruders. The sequence of above steps will depend on your organization's specific needs and responsibilities under federal, state, local, and international law.

EXECUTE

N. Assess the incident:

Immediately assess the nature and scope of the incident, to determine whether the incident was caused by a malicious act, human error, a technological glitch, or a combination of those factors. This step will define the type of assistance needed to mitigate the specific damage. Do not switch off power to the affected network or device. If your organization's network has appropriate logging capabilities, a system administrator can attempt to identify the affected computer systems, apparent origin of the incident, any malware used, and/or any remote servers where data was transferred. Additionally, this step will enable documenting which users are logged onto the network, which processes are running, current external connections to computer systems, and all open ports and associated services and applications. Ensure that your organization does not unintentionally or unnecessarily modify stored data, which can hinder IR and the investigation.

O. Implement protective measures:

To prevent further damage, begin implementing the protective measures outlined in the IR Plan, while maintaining detailed records of the steps taken to mitigate the damage. This information may be used later to establish criminal violations and recover remediation costs from the intruders, dependent on federal, state, local, and international law.

P. Document the response:

Direct the IR Team and IR firm personnel to keep a contemporaneous written record of all steps undertaken, to assist the investigation and reconstructing the order of events. Record the descriptions, dates and times of all incident-related events, incident-related phone calls, emails, and other contact, along with the identity, roles, and responsibilities of IR personnel (internal and contracted) performing tasks related to the incident. Include technical information, such as the identity of systems, accounts, services, data, and networks affected by the incident. Other information to include is the amount and type of damage inflicted, information regarding network topology, type and version of software being run on all affected systems, and any peculiarities in the organization's network architecture, such as proprietary hardware or software. Document and save communications relating to the incident, in particular threats, claims of credit, extortion demands, suspicious calls, emails, or other requests for information about the incident.

Q. Preserve evidence:

Typically, a cyber incident is a result of a malicious (criminal) action, and therefore a crime scene that needs to be preserved. Some examples of evidence to preserve and document include, previously maintained server logs (firewall, event and active directory), an up-to-date network map that includes authorized remote connections, a list of affected servers, disk images, memory images, communications from intruders, screenshots and copies of malware, ransomware and any other relevant information. A timeline of events is crucial in reconstructing the incident and preparing the preserved evidence for investigation and prosecution.

Consider imaging the affected systems using forensically sound procedures to preserve a record at the time of the incident for later analysis and potentially for use as evidence at trial. A forensic image is an exact, bit-for-bit copy of data of an electronic device, and provides a snapshot of the system at the time the image was created, including deleted files, slack (apparently empty) storage space, system files, and executable files. Protect the media by restricting access to ensure that it is not altered, and document who has maintained possession of the media to establish a chain-of-custody.

When using regularly generated backups, ensure that they are isolated from the affected systems and check them on isolated computers prior to using them to restore the system. Intrusions are commonly only discovered long after an initial intrusion occurred, and may require the retrieval of old backups to pre-date the intrusion. Isolated backups are particularly critical in mitigating ransomware attacks.

R. Contact law enforcement:

If there is suspicion that the cyber incident is a result of criminal activity, contact law enforcement as predetermined in the IR Plan. Once this contact is established, share forthcoming press releases regarding the incident with the investigators before releasing information that might impede the investigation. Having established liaison with law enforcement will streamline this step by clarifying what entities your organization should contact and when. Becoming a member of a Secret Service CFTF and having followed the steps outlined in this guide should have prepared your organization. Some organizations assume that contacting a law enforcement agency, such as the Secret Service, will publicize the incident and make the organization subject to civil lawsuits. When it comes to civil litigation the Secret Service is subject to Federal Court subpoenas, but not state or local court jurisdiction. Additionally, information concerning ongoing criminal investigations is subject to strict internal policies and Department of Justice regulations that govern federal law enforcement.

S. Contact regulators:

Depending on the type of incident, and if required, contact regulatory agencies as predetermined in the IR Plan. This is an important step in your organization's response to a cyber incident. Proper execution of this step of the IR Plan largely depends on your organization understanding its responsibilities regarding data protection and data breach reporting under federal, state, local, and international law.

The Secret Service, similar to other federal law enforcement agencies, is not mandated to notify regulators, and criminal investigators are focused on deterrence and apprehension of criminals. Furthermore, federal government agencies are independent of each other and information sharing among them is subject to the **Privacy Act of 1974.**

DEBRIEF

T. Continue monitoring:

After a cyber incident appears to be under control, continue monitoring systems for anomalous activity. Remain vigilant for new signs of re-infection and compromise.

U. Notify other organizations:

If there is evidence that the cyber incident has affected another organization, notify the organization. If this incident is being investigated by law enforcement, the notification may need to be issued by them to maintain the integrity of a potential criminal case. Additionally, the Cybersecurity Information Sharing Act of 2015 (CISA) enabled organizations to participate in the exchange of cyber threat indicators with the Federal Government though the **DHS Automated Indicator Sharing (AIS).**

V. Conduct a post-incident review:

Review the performance of the incident response and note the deficiencies and gaps in executing the IR Plan, to include determining if each step in the plan was followed or why not. Assess the roles and responsibilities of the members of the IR Team, and if applicable, the IR firm and the legal experts.

W. Adjust the IR Plan:

Address shortcomings in security practices according to the findings of the post-incident performance review. Adopt measures to prevent similar attacks in the future, consider acquiring resources to better secure its systems. Adjust the roles and responsibilities of the IR Team and other participants of the incident response.

Further resources:

www.secretservice.gov/investigation U.S. Secret Service Criminal Investigations

www.nist.gov/topics/cybersecurity U.S. National Institute of Standards and Technology

www.dhs.gov/be-cyber-smart U.S. Department of Homeland Security Cyber-Smart Campaign

www.justice.gov/criminal-ccips U.S. Department of Justice Computer Crime and Intellectual Property Section

www.cisa.gov/about U.S. Dept. of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)

www.ice.gov/hsi U.S. Department of Homeland Security Homeland Security Investigations

www.fbi.gov/investigate/cyber U.S. Federal Bureau of Investigation

www.ftc.gov U.S. Federal Trade Commission

www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business
U.S. Federal Trade Commission, Data Breach Response: A Guide for Business

https://enterprise.verizon.com/resources/reports/dbir Verizon Data Breach Investigations Reports

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02016R0679-20160504
European Union General Data Protection Regulation

www.enisa.europa.eu European Union Agency for Cybersecurity

www.pcisecuritystandards.org Payment Card Industry (PCI) Security Standards Council

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

BEFORE AN INCIDENT

UNDERSTAND

A. Establish liaison and partnerships
B. Study the legal framework
C. Understand legal responsibilities
D. Maintain cyber awareness

PREPARE

E. Determine vulnerabilities
F. Prioritize and institute cybersecurity measures
G. Monitor the network
H. Develop policies and conduct training
I. Develop a communication strategy
J. Consider retaining legal services
K. Consider retaining incident response (IR) services
L. Prepare for evidence preservation
M. Create an IR Plan

DURING AN INCIDENT

EXECUTE

N. Assess the incident
O. Implement protective measures
P. Document the response
Q. Preserve evidence
R. Contact law enforcement
S. Contact regulators

AFTER AN INCIDENT

DEBRIEF

T. Continue monitoring
U. Notify other organizations
V. Conduct a post-incident review
W. Adjust the IR Plan

◀ BACK

APPENDIX E

TEXAS DEPARTMENT OF INFORMATION RESOURCES

Incident Response Team Redbook

June 2020

Contents

Introduction 3

SECTION 1 Glossary and Acronyms 4
- 1.1 Glossary 4
- 1.2 Common Acronyms 8

SECTION 2 Incident Response Policy 10
- 2.1 Sample Security Incident Response Policy 10

SECTION 3 Privacy/Security Event Initial Triage Checklist 12

SECTION 4 Event Threat, Impact Analysis, and Escalation Criteria 13
- 4.1 Event Threat and Impact Analysis 13
- 4.2 Event Escalation: Communication 14

SECTION 5 Breach Notice Criteria 16

SECTION 6 Post-Incident Checklist 20

SECTION 7 Incident Response Team Templates 21
- 7.1 Title and Contact Information for Plan Sponsor/Owner 22
- 7.2 IRT Charter 23
- 7.3 IRT Membership by Roles 25
- 7.4 IRT Meeting Minutes 27
- 7.5 IRT Action List 28
- 7.6 IRT State Government Contact Information 29

SECTION 8 Additional Templates 30
- 8.1 Identity Theft Protection Criteria 31
- 8.2 Internal Management Alert Template 33
- 8.3 Notice to Individuals Affected by Incident 34
- 8.4 Public (Media) Notice 37
- 8.5 Post-Mortem and Improvement Plan 37

SECTION 9 External Contacts 38
- 9.1 State of Texas Contacts 38
- 9.2 Federal Contacts 39
- 9.3 Industry Contacts 40
- 9.4 Press Contacts 42

SECTION 10 Legal References 43
- 10.1 Texas Laws and Regulations for Data Privacy and Security 43
- 10.2 Federal Laws and Regulations for Data Privacy and Security 45
- 10.3 Other Laws and Regulations for Data Privacy and Security 49

Acknowledgements 50

Introduction

When a privacy or information security incident occurs, it is imperative that the agency follow documented procedures for responding to and processing the incident. An Incident Response Team (IRT) Redbook is intended to contain the procedures and plans for such incidents when they occur. The Redbook should be in both hard copy and electronic formats and be readily available to any standing member of the IRT team.

Two principles guide the establishment of the Redbook. First, is that every agency must establish in advance and maintain a plan for responding to an incident. Second, every agency must test and update the operation of the plan periodically to ensure that it is appropriate and functional.

This is a template and is intended to be a framework for state agencies in creating their own Redbook and should be modified and completed to meet the business needs of the agency.

Defined terms are in **bold** print.

SECTION 1

Glossary and Acronyms

1.1 Glossary

Admissible Evidence: evidence that is accepted as legitimate in a court of law, *see* Chain of Custody.

Authentication: security measure designed to establish the validity of a transmission, message, or originator, or the identity confirmation process used to determine an individual's authorization to access data or computer resources.

Authorized User: a person granted certain permissions to access, manage, or make decisions regarding an information system or the data stored within.

Authorized Use and Disclosure: a permissible action or use of **Confidential Information**.

Authorization: the act of granting a person or other entity permission to use data or computer resources in a secured environment.

Availability: The security objective of ensuring timely and reliable access to and use of information.

Breach: an impermissible use or disclosure by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of **Confidential Information** such that the use or disclosure poses a significant risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Depending upon applicable law, "Breach" may for example mean:

1) HIPAA Breach of Protected Health Information ("PHI"). With respect to PHI pursuant to HIPAA Privacy and Breach Notification Regulations and regulatory guidance any unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Regulations is presumed to be a Breach unless a Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Compromise will be determined by a documented Risk Assessment including at least the following factors:
    a. The nature and extent of the **Confidential Information** involved, including the types of identifiers and the likelihood of re-identification of PHI;
    b. The unauthorized person who used or to whom PHI was disclosed;
    c. Whether the Confidential Information was actually acquired or viewed; and
    d. The extent to which the risk to PHI has been mitigated.

    With respect to PHI, a "Breach" pursuant to HIPAA Breach Regulations and regulatory guidance *excludes*:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority, and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations.
    b. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate location to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement as

defined by HIPAA in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations

c. A disclosure of PHI where a Covered Entity or Business Associate demonstrates a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, pursuant to HIPAA Breach Regulations and regulatory guidance.

2) Breach in Texas. Breach means "Breach of System Security," applicable to electronic Sensitive Personal Information (SPI) as defined by the Texas Identity Theft Enforcement and Protection Act, Business and Commerce Code Ch. 521, that compromises the security, confidentiality, or integrity of Sensitive Personal Information. Breached SPI that is also PHI may also be a HIPAA breach, to the extent applicable.
3) Any unauthorized disclosure as defined by any other law and any regulations adopted thereunder regarding **Confidential Information**.

Business Continuity Plan: the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Chain of Custody: refers to the application of the legal rules of evidence and its handling.

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. This includes any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) that consists of or includes any or all of the following:

1) Federal Tax Information, sourced from the Internal Revenue Service (IRS) under an IRS data sharing agreement with the agency;
2) Personal Identifying Information;
3) Sensitive Personal Information;
4) Protected Health Information, whether electronic, paper, secure, or unsecure;
5) Social Security Administration data, sourced from the Social Security Administration under a data sharing agreement with the agency;
6) All non-public budget, expense, payment, and other financial information;
7) All privileged work product;
8) Information made confidential by administrative or judicial proceedings;
9) All information designated as confidential under the laws of the State of Texas and of the United States, or by agreement; and
10) Information identified in a contract or data use agreement to which an agency contractor specifically seeks to obtain access for an Authorized Purpose that has not been made public.

Confidentiality: The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Containment: the process of preventing the expansion of any harmful consequences arising from an Incident.

Contingency Management Plan: a set of formally approved, detailed plans and procedures specifying the actions to be taken if or when particular circumstances arise. Such plans should include all eventualities ranging from key staff absence, data corruption, loss of communications, virus infection, partial loss of

system availability, etc.

Data: information in an oral, written, or electronic format that allows it to be retrieved or transmitted.

Disaster Recovery Plan: a crisis management master plan activated to recover IT systems in the event of a disruption or disaster. Once the situation is under control, a Business Continuity Plan should be activated.

Discovery: the first time at which an event is known, or by exercising reasonable diligence should have been known, by an officer, director, employee, agent, or agency contractor, including events reported by a third party to an agency or agency contractor.

Encryption: The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning. Applicable law may provide for a minimum standard for compliant encryption, such as HIPAA or NIST standards.

Eradication: the removal of a threat or damage to an information security system.

Event: an observable occurrence in a network or system.

Forensics: the practice of gathering, retaining, and analyzing information for investigative purposes in a manner that maintains the integrity of the information.

Hardware: the physical technology used to process, manage, store, transmit, receive, or deliver information. The term does not include software. Examples include laptops, desktops, tablets, smartphones, thumb drives, mobile storage devices, CD-ROMs, and access control devices.

Harm: although relative, the extent to which a privacy or security incident may actually cause damage to an agency or harm to an individual, reputation, financial harm, or results in medical identity theft.

Incident: an event which results in the successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.

Incident Response Lead: person responsible for the overall information security Incident management within an agency and is responsible for coordinating the agency's resources which are utilized in the prevention of, preparation for, response to, or recovery from any Incident or Event.

Incident Response Team (IRT): led by the Incident Response Lead, the core team composed of subject-matter experts and information privacy and security staff that aids in protecting the privacy and security of information that is confidential by law and provides a central resource for an immediate, effective, and orderly response to Incidents at all levels of escalation.

Information Security: the *administrative, physical,* and *technical* protection and safeguarding of data (and the individual elements that comprise the data).

Integrity: The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity

Local Area Network (LAN): a private communications network owned and operated by a single organization within one location.

Malicious Code: a software program that appears to perform a useful or desirable function but actually gains unauthorized access to computer system resources or deceives a user into executing other malicious logic.

Malware: a generic term for different types of malicious code.

Penetration: gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Protected Health Information (PHI): information subject to HIPAA. Individually identifiable health information in any form that is created or received by a HIPAA Covered Entity, and relates to the individual's healthcare condition, provision of healthcare, or payment for the provision of healthcare as further described and defined in the HIPAA Privacy Regulations. PHI includes:

- demographic information unless such information is De-identified as defined in the HIPAA Privacy Regulations;
- "Electronic Protected Health Information" and unsecure PHI as defined in the HIPAA Privacy Regulations;
- the PHI of a deceased individual within 50 years of the date of death; and
- employment information.

Personal Identifying Information (PII): as defined by the Texas Business and Commerce Code §521.002(a)(1), "personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

- name, social security number, date of birth, or government-issued identification number;
- mother's maiden name;
- unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- unique electronic identification number, address, or routing code; and
- telecommunication access device as defined by the Penal Code §32.51.

Privacy: the right of individuals to keep information about themselves to themselves and away from others. For example, privacy in the healthcare context means the freedom and ability to share an individual's personal and health information in private.

Protocol: a set of formal rules describing how to transmit data, especially across a network.

Recovery: process of recreating files which have disappeared or become corrupted from backup copies.

Reportable Event: an event that involves a breach of Confidential Information requiring legal notification to individuals, government authorities, the media, or others.

Risk Assessment: the process by which the potential for harm is identified and the impact of the harm is determined. The process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Sensitive Data: while not necessarily protected by law from use or disclosure, data that is deemed to require some level of protection as determined by an individual agency's standards and risk

management decisions. Some examples of "Sensitive Data" include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Internal communications
- Information determined to be authorized for use or disclosure only on a "need-to-know" basis

Sensitive Personal Information (SPI: as defined by the Texas Business and Commerce Code §521.002(a)(2) means:

1) An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or
    c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
2) Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health care to the individual.

The term "Sensitive Personal Information" does not include publicly available information that is lawfully made available to the public from the federal, state, or local government.

Server: a processor computer that supplies a network of less powerful machines (such as desktop PCs and laptop computers) with applications, data, messaging, communication, information, etc.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

Vulnerability: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Wide Area Network (WAN): a communications network that extends beyond the organization's immediate premises.

1.2 Common Acronyms

CDO: Chief Data Officer

CFAA: Computer Fraud and Abuse Act (1986)

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CJIS: Criminal Justice Information Services, a division of the FBI

CLIA: Clinical Laboratory Improvement Amendments

CPO: Chief Privacy Officer

CTO: Chief Technology Officer

FERPA: Family Educational Rights and Privacy Act (1974)

FISMA: Federal Information Security Management Act (2002)

FTI: Federal taxpayer information

HIPAA: Health Insurance Portability and Accountability Act (1996)

HITECH Act: Health Information Technology for Economic and Clinical Health Act (2009)

IRS: Internal Revenue Service

IRT: Incident Response Team

ISO: Information Security Office

IT: Information Technology

NIST: National Institute of Standards and Technology

PHI: Personal Health Information

PIA: Public Information Act, Government Code Ch. 552

PII: Personal Identifying Information

SPI: Sensitive Personal Information

SSA: Social Security Administration

TAC: Texas Administrative Code

SECTION 2

Incident Response Policy

Each agency should have a policy to address compliance with privacy and security breach management. Below is a sample policy which should be replaced by each agency and should be consistent with the agency's incident response plan.

2.1 Sample Security Incident Response Policy

Purpose

The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with the Texas Administrative Code, Title 1, Chapter 202. This document sets forth the policy for incident management within the Agency.

Scope

This policy applies to and must be complied with by all Agency Users.

The User agrees to abide by this policy while employed or contracted with the Agency.

Roles and responsibilities of each function pertaining to the protection of Agency-owned systems and data are documented in Agency policy.

The User is responsible for understanding the terms and conditions of this policy.

Exemptions to this policy shall follow the process defined in Agency policy.

This policy is subject to change.

This policy applies to any computing device owned or leased by the Agency. It also applies to any computing device regardless of ownership, which either is used to store Agency-owned Confidential or Agency-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.

Policy

The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Information Resources Manager (IRM) for approval. 1 TAC §202.26

The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that fall under one or the following categories: 1 TAC §202.26

- Propagation to external systems
- Violation of applicable federal and/or state laws which will require involvement from law enforcement

- Potential modification or disclosure of Confidential Information as defined in the Agency Data Classification Policy.

The Agency shall notify appropriate individuals (which must include the State CISO and the State Cybersecurity Coordinator) within 48 hours if it is believed that personal information owned by the Agency has been used or disclosed by or for unauthorized persons or purposes. — TGC §2054.1125, TBC §521.053

The ISO shall establish an Incident Criticality matrix. This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants. — 1 TAC §§202.21-22

The ISO shall establish and document appropriate procedures, standards, and guidelines regarding Incidents. — 1 TAC §202.21

The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by the Agency may be subject to seizure and retention by the ISO.

The Chief Information Security Officer, Chief Privacy Officer, or Agency General Counsel (as appropriate) will work directly with law enforcement regarding any Incidents that may have violated federal or state laws. If an Incident is determined to be the result of a privacy violation by a User, the ISO shall notify the User's supervisor and Human Resources of the violation(s), or the Inspector General's Office, as applicable, for appropriate action.

The ISO shall provide a summary report for each valid Security Incident to the IRM within five business days after the incident has been closed.

Disciplinary Action

Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law.

Any User who has violated this policy may be subject to disciplinary action, up to and including termination of employment or contract with DIR.

The Agency will cooperate with appropriate law enforcement if any User may have violated federal or state law.

Document Change Management

All changes to this document shall follow the process defined in Agency policy.

The ISO will be responsible for communicating the approved changes to the organization. — 1 TAC § 202.21

SECTION 3

Privacy/Security Event Initial Triage Checklist

1) **Incident Response Team:** Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident. Meet daily if necessary, with priority over other work, possibly requiring after-hours activities.

2) **Secure data:** Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate, e.g. harden or disable system or contact internet search engines if appropriate to clear internet cache.

3) **Data elements:** Determine the types, owners, and amounts of confidential information that were possibly compromised.

4) **Data source:** Identify each location where confidential information may have been compromised and the business owner of the confidential information.

5) **Scope and escalation:** Confirm the level and degree of unauthorized use or disclosure (includes access) by the named or unidentified individuals or threats.

6) **Number of individuals impacted:** Determine the number of individuals impacted. The number may implicate breach notification requirements, e.g. individual or media notice.

7) **Discovery date:** Determine the date the agency or contractor knew or should have known about the event/incident.

8) **Management alert:** Advise appropriate internal management.

9) **External communications, as required:** Advise external contacts, such as DIR, legislative leadership, the Office of the Inspector General, the Office of the Attorney General, Secretary of State (SOS) (if election data involved), law enforcement, outside counsel, and applicable regulatory authorities.

10) Investigate:

   a. Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.

   b. Documents: Gather and review contracts and provisioning documents (documents authorizing access or restricting use or disclosure).

   c. Root Cause Analysis: Prepare RCA which describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence.

   d. Event and Threat Impact Analysis (see section on Event Threat and Impact Analysis below).

11) **Mitigation:** Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence. Set timeline and assign responsibility to ensure accountability. Follow-up to ensure corrective action initiated and completed on time or decision to accept the risk of reoccurrence, and report appropriately.

SECTION 4

Event Threat, Impact Analysis, and Escalation Criteria

The investigation of the incident/event should include an Event Threat and Impact Analysis to accurately categorize the impact of the event on the organization. Once the event's impact level is understood it may be appropriate to escalate the incident response and contact other entities.

4.1 Event Threat and Impact Analysis

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include:

- **Functional Impact.** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.
- **Information Impact.** Incidents may affect the confidentiality, integrity, and availability of the organization's information.
- **Recoverability.** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

While there is no single model for determining event impact, the below tables provide guidance on defining impact to organization systems, organization information (business impact), and organization ability to recover from an event (possible responses). Organizations should consider each category to assure proper response and recovery from these events.

Table 4.1: Examples of functional impact categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

Table 4.2: Examples of possible information impact categories

Category	Definition
None	No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised.
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes.
Integrity Loss	Sensitive or proprietary information was changed or deleted accidentally or intentionally.

Table 4.3: Examples of recoverability effort categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation.

4.2 Event Escalation: Communication

NIST 800-61 Computer Security Incident Handling Guide provides advisement on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications.

Key Contacts. Organizations should establish an escalation process for instances when key individuals outside of normal technical response processes must be notified. Among those to be considered are:

- CIO or Information Resources Manager (IRM)
- CISO or Information Security Officer (ISO)
- CPO or Privacy Officer
- Other incident response teams within the organization
- External (contractor) incident response teams, if appropriate
- System owner
- Human resources
- Public affairs
- Legal department
- US-CERT (required for systems operated on behalf of the federal government)

- Law enforcement, if appropriate
- Federal government agencies, if appropriate
- Department of Information Resources Office of the CISO (Mandated for Texas Agencies)

Contact Methods. Organizations may need to provide status updates to certain external and internal parties. Among communication methods to be considered are:

- Email
- Website (internal, external, or portal)
    - Note: The official State Portal to notify DIR is SPECTRIM and all ISOs have access to this system
- Telephone calls
- In person (e.g., daily briefings)
- Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting)
- Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

SECTION 5

Breach Notice Criteria

Certain types of breaches carry legal notification responsibilities. This section includes information about breach notification statutes and rules according to Texas law, federal laws and regulations, and other states' laws. ***NOTE*** As of 9/1/2017 TGC §2054.1125 requires notification of the Texas Office of the Chief Information Security Officer and the State Cybersecurity Coordinator within 48 hours of discovery for all Breaches (actual or suspected) which require disclosure by law or agreement. For any Breach involving Election Data, the Office of the Secretary of State must be notified.

Table 5.1: Texas legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
Texas Identity Theft Enforcement and Protection Act (2005) Updated 2019	Texas Business and Commerce Code Ch. 521, §521.053	Report any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person or to the data owner immediately. Public reports may be required for breaches involving 10,000 or more individuals. An organization that is required to disclose or provide notification under this section, is required to notify the Texas Attorney General if the breach involves at least 250 Texas residents. This notification must include: 1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach; 2. The number of residents of this state affected by the breach at the time of notification; 3. The measures taken by the person regarding the breach; 4. Any measures the person intends to take regarding the breach after the notification under this subsection; and 5. Information regarding whether law enforcement is engaged in investigating the breach.	Government Code §2054.1125 makes Business and Commerce Code §521.053 applicable to state agencies.

Table 5.2: Federal legal requirements for breach notices

Breach Notice	Citation	Requirement	Notes
HIPAA	45 CFR §164.404	Notify individual or Covered Entity of a breach of unsecured protected health information which poses a significant risk of financial, reputational, or other harm to the individual. Individual notice must contain certain mandatory media notices (involving 500 or more individuals) as soon as possible but no later than 60 days from discovery of the breach.	Applies only to HIPAA Covered Entities and HIPAA-protected health information. A Business Associate of a Covered Entity is required to notify the Covered Entity as soon as possible but no later than 60 days from the discovery of the breach. Contracting for a shorter time is a best practice.
Federal Financial Participation	CMS SMDL #06-022	CMS-regulated entities must notify CMS within one clock hour according to Sep. 2006 CMS letter to State Medicaid Directors	Unclear if HIPAA HITECH eliminated the CMS requirement. SNAP, TANF, and CHIP each have similar authorizations to use or disclose Medicaid information that identifies an applicant or

			recipient is limited to use or disclosure "directly in connection with program administration," but have no breach notice requirement.
Internal Revenue Service	By data sharing agreement with the IRS, pursuant to IRS Publication 1075 §10	Notify TIGTA and IRS Office of Safeguards of compromised IRS or SSA data within one clock hour from discovery of an actual or suspected breach. Follow individual agency procedures for notifying impacted individuals.	The IRS Office of Safeguards may require individual notification.
Social Security Administration (SSA)	By contract between SSA and Agency which defers to IRS Publication 1075	Notice required to SSA within one clock hour of discovery. Follow instructions of SSA to notify impacted individuals, if any.	SSA may require individual notification.
Federal Trade Commission (FTC)	Health Breach Notification (PHR, EHR Vendors) 16 CFR Part 318	Requires a vendor of personal health records to notify the individual US Citizen and the FTC following the discovery of a breach of security of unsecured PHR-identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR-related entity.	Applies to foreign and domestic vendors of personal health records, PHR-related entities, and third-party service providers, irrespective of any jurisdictional tests in the FTC Act, that maintain information of US citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. "Breach" is acquisition unauthorized by the individual. Notify without unreasonable delay and in no case later than 60 calendar days after the breach discovery.
Family Educational Rights and Privacy Act (1974)	20 USC §1232g, 34 CFR Part 99	None. FERPA guidance recommends having breach response plans.	Applies to educational institutions regarding the privacy of personally identifiable information contained in education records of students. Consent is generally required to disclose education records.

State Data Breach Notification Laws: The National Conference of State Legislatures maintains a matrix of state data breach laws. As of April 2019, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

Table 5.3: Security breach notification statute in other states, Texas, and territories (NCSL)

State	Citation
Alabama	2018 S.B. 318, Act No. 396
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-545
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82 & Cal. Civ. Code §§ 1798.100 - 1798.199
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-439 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 *et seq.*
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. § 51:3071 *et seq.*
Maine	Me. Rev. Stat. tit. 10 § 1346 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.,* Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 252E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 356-C:19, -C:20, -C:21
New Jersey	N.J. Stat. § 56:8-163
New Mexico	N.M. 2017 H.B. 15, Chap. 36
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat. §§ 75-61, 75-65
North Dakota	N.D. Cent. Code § 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166

Oregon	Oregon Rev. Stat § 646A.600 *et seq.*
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws § 11-49.3-1 *et seq.*
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-20 to -46 (2018 S.B. 62)
Tennessee	Tenn. Code § 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053, Tex. Ed. Code § 37.007(b)(5)
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 § 2430, 2435
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05
Washington	Wash. Rev. Code § 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 *et seq.*
Wisconsin	Wis. Stat § 134-98
Wyoming	Wyo. Stat. § 40-12-501 *et seq.*
District of Columbia	D.C. Code § 28-3850 *et seq.*
Guam	9 GCA § 48-10 *et seq.*
Puerto Rico	10 Laws of Puerto Rico § 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14 § 2208

SECTION 6

Post-Incident Checklist

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Per section 3.4.1 (Lessons Learned) and section 3.4.2 (Using Collected Incident Data) relevant factors for post-incident and root cause analysis include:

1) **Learning and improving.** Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
    a. Exactly what happened, and at what times?
    b. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
    c. What information was needed sooner?
    d. Were any steps or actions taken that might have inhibited the recovery?
    e. What would/should staff and management do differently the next time a similar incident occurs?
    f. How could information sharing with other organizations have been improved?
    g. What corrective actions can prevent similar incidents in the future?
    h. What precursors or indicators should be watched for in the future to detect similar incidents?
    i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

2) **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
    a. Creating a formal event chronology (including time-stamped information from systems);
    b. Compiling a monetary estimate of the amount of damage the incident caused;
    c. Retaining follow-up reports as specified in retention policies.

3) **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.

4) **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
    a. Reviewing of logs, forms, reports, and other incident documentation;
    b. Identifying recorded precursors and indicators;
    c. Determining if the incident caused damage before it was detected;
    d. Determining if the actual cause of the incident was identified;
    e. Determining if the incident is a recurrence of a previous incident;
    f. Calculating the estimated monetary damage from the incident;
    g. Measuring the difference between initial impact assessment and the final impact assessment; and
    h. Identifying measures, if any, that could have prevented the incident.

SECTION 7

Incident Response Team Templates

Included in this section are templates relevant to the operation of an Incident Response Team: the title and contact page for the plan's sponsor/owner, a sample charter, a membership list that lists important roles, an example record of meeting minutes, a post-meeting action list, and a list of important state government contact information. The plan sponsor or owner is responsible for modifying these templates for the incident response team's purposes. Brackets indicate where the IR Lead should customize to reflect the agency.

7.1 Title and Contact Information for Plan Sponsor/Owner

[Agency Name]

Information Privacy or Security Incident Response Team Redbook

For questions or further information, please contact:

	Name	Phone	Email
Sponsor			
Owner			

"Sponsor" is the executive responsible for compliance
"Owner" is the owner of this document

7.2 IRT Charter

Information Privacy or Security Incident Response Team Charter

Charter Purpose:

This Incident Response Team (the "IRT") Charter establishes membership, subject matter experts, roles, responsibilities, and activities of the [agency] IRT to respond to an actual or suspected information privacy or security event/incident.

IRT Mission:

The IRT mission is, first, to prevent incidents by reasonably anticipating, detecting, and planning for actual and suspected privacy or security events; and second, to respond to and mitigate privacy or security events.

Overview:

The Incident Response Team (the "IRT") is a standing team of internal personnel established by [Executive Management] in this [Charter] with expertise in responding to a significant actual or suspected privacy or security event or incident. The IRT operates on behalf of [Executive Management] and engages, informs, and receives support from [Executive Management]. There [is/is not] a set protocol to initiate the IRT activities in response to an actual or suspected event/incident. Once activated, the IRT has authority to [request cooperation/establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours].

Responsibilities and Roles:

Responsibilities:

1) **Anticipate and prepare** [the agency] for privacy or security events/incidents which can be reasonably anticipated;
2) **Respond** to actual or suspected events/incidents on behalf of [the agency] as needed, with activities such as:
    a. Triage (see section 2);
    b. Communication, internal and external, as needed according to [agency's] communications protocol (e.g. funneled to the top from a deputy, for example) (see communications templates)
    c. Track and document IRT activities and discoveries; and
    d. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

- Uncontained or escalating malware attack on system (computer virus, worm, bot, or Trojan);
- Abuse, theft, misuse, or loss of data or hardware (including unauthorized use, disclosure, or access to computer accounts, systems, or data; hacking; human error);

- Improper use or disclosure of information or information resources as outlined in [agency] standards or contracts including e-mail, equipment, Internet, and acceptable data use (includes human resources or contractor misuse or error);
- Many individuals or a large amount of sensitive data impacted; or
- Events likely to be high-profile or create a significant risk of individual harm (e.g., risk of financial harm, reputational harm, or medical identity theft).

Roles:

1) **The IRT Lead.** The Lead of the IRT may:
    a. Be designated by and reporting to [Executive management]. The IRT is led by [_____] or his or her designee.
    b. Declare an incident
    c. Establish, maintain, and update written IRT protocols or incident response plans
    d. Identify roles and responsibilities for IRT standing members
    e. Request or designate ad hoc members for particular events as needed
    f. [request cooperation / establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours]

2) **IRT Standing Members.** The standing members include named individuals or representatives.

3) **Ad hoc Members or Subject Matter Experts.** Ad hoc members or Subject Matter Experts may be designated as ad hoc resources by the IRT Lead.

7.3 IRT Membership by Roles

The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

Standing IRT Membership Contact Information - *Confidential*

Standing Members	Name	Phone	Email	After-hours contact
IRT Lead				
[Chief Information Officer or designee]				
[Chief Information Security Officer or designee]				
[Information Resources Manager or designee]				
[Internal Audit]				
[Office of Inspector General]				
[Other]				
[Other]				
[Other]				
Legal Counsel to the IRT – to avoid losing attorney-client privilege, *do not list legal as a member*				

Ad Hoc IRT Members

Ad hoc Members	Name	Phone	Email	After-hours contact
[Relevant business area, department, division]				
[Communications]				
[External Relations]				
[Open Records]				
[Third parties, e.g., contractor]				
[Department of Information Resources designee]				

[Counsel, Office of Attorney General]				
[Vendor for Breach Management services]				
[Law Enforcement]				
[Outside legal counsel]				
[Other]				
[Other]				
[Other]				

Note 1: Standing members are relatively static; ad hoc members are designated for each incident.
Note 2: After hours contact information is critical to incident handling.

7.4 IRT Meeting Minutes

CONFIDENTIAL

Meeting Minutes for [Agency] IRT Meeting____, 20__

Purpose: The purpose of this message is to provide updates regarding the IRT activities in response to confirmed privacy and/or security incidents involving personal or confidential information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action. This Alert will be regularly updated as more information becomes available.

Summary
Brief incident summary:
Participants
IRT Members Present: *IRT Members Not in Attendance:* *Guests:*
Current Updates
1. 2. 3.
Prior Updates
1. 2. 3.
Next Steps
1. 2.
Next Scheduled Meeting

__:00, _. m.,____.____, 20__
Location:
Conference No.:_____Access Code: _____

7.5 IRT Action List

IRT: Identification Name or Number

Action Items Status

Current Updates as of____. __,20__

Item	Date	Action	Assigned To	Status
1.				
2.				
3.				
4.				
5.				
6.				

7.6 IRT State Government Contact Information

IRT State Government Contact Information

Entity	Contact	Division/Location	Email/Office Telephone
Office of the Governor			
Lieutenant Governor			
Speaker of the House			
State of TX Office of the Chief Information Security Officer			
State Cybersecurity Coordinator			
[Agency Board or Commission Chair]			
[Agency Oversight Senate Committee Chair]			
[Agency Oversight House Committee Chair]			

SECTION 8

Additional Templates

Included in this section are additional guidelines and templates which may be of use to the Incident Response Team: the Identity Theft Protection Criteria, a sample Internal Management Alert, a sample Notice to Individuals Affected by Incident, and a Public (Media) Notice. The plan sponsor or owner is responsible for modifying these templates to fit the IRT's purpose. Brackets indicate where the IR Lead should customize the template to reflect the agency's needs.

8.1 Identity Theft Protection Criteria

Although it is optional for a state agency to provide identity theft protection, each agency should evaluate the risk of financial or medical identity theft occurring. If the risk is deemed significant, the agency may consider this type of protection. In addition to deciding whether to provide the protection, an agency should consider an appropriate length of time to provide the protection. Ultimately the decision to provide protection should be made at an Executive-level position. Should an agency determine identity theft protection is appropriate, there are various types and level of protection to choose from on the market, including:

- Identity theft insurance with various coverages or guarantees
- Credit report monitoring
- Claims monitoring
- Monitoring of websites used to trade stolen information
- Theft assistance resolution

DIR has contracts with one or more vendors of identity theft amelioration services. As noted, commercial identity theft protection varies in the means and extent of coverage. While some carriers offer compensation for expenses incurred as a result of theft, others simply provide credit monitoring and alerts to an individual in the event of credit activity. In addition to assistance for affected individuals, breach management services can be procured to assist an entity responsible for a breach, as well as provide risk assessment, mitigation, or remediation services. As circumstances warrant, [Agency] may elect to procure commercially available identity theft protection or breach management services, especially for high-profile events likely to lead to significant harm to impacted individuals or reputational harm or cost to [Agency].

[Agency] will consider the following criteria to determine whether to procure identity theft protection or breach management services:

1) Contract opportunities made available to state agencies by the Department of Information Resources for identity theft or breach management services [see resources page].
2) Contractual requirements imposed upon the [Agency] vendor or contractor, or other third party responsible for the breach, to provide identity theft protection, breach management services to the agency, or any other indemnification or hold harmless contract provisions.
3) Degree and scope of the breach and the degree or type of risks to individuals, such as financial, reputational, or other harm (such as medical identity theft or criminal identity theft), dependent upon the various forms of identity theft.
4) The extent to which commercial services will be unable to detect or deter harm such as medical or criminal identity theft for the breach at issue.
5) No or low-cost measures available to impacted individuals to protect themselves, such as a self-imposed credit fraud alert, a credit freeze request to one of the credit bureaus [see breach notice template for more information], or filing a police report. Some options for impacted individuals include:
    a. A **fraud alert** which can help prevent an identity thief from opening additional accounts in a consumer's name in 90 days.

b. A **security freeze**, also known as a **credit freeze**, which is a warning sign to businesses or others who may use an individual's credit file and requires a police report.
c. Contacting the **Consumer Protection Division** of the Texas Office of the Attorney General.

6) The ability to link the breach event to an identity theft event or other harm.
7) The cost to the agency or agency contractor for the provision of identity theft or breach management services.

8.2 Internal Management Alert Template

NOTICE: The information contained in this message and any attachment to this message are confidential under state or federal law and may be protected by attorney-client privilege. If you have received this message in error, please immediately notify the sender of this e-mail, then delete or destroy it and any attachment(s). Thank you.

Agency Data Security Incident Alert

Purpose: The purpose of this message is to inform you of a suspected or confirmed privacy and/or security incident involving personal information that is protected by state and/or federal law. This alert provides up-to-the-moment information and recommendations for immediate action and will be regularly updated as more information becomes available.

Summary
Brief incident summary:
Immediate Recommendations:
1. 2. 3.
Next Steps:
1. 2. 3.
Next Scheduled Update:
[Time/Day/Date or "As conditions warrant"]

8.3 Notice to Individuals Affected by Incident

<Date>

<<Title>> <<First Name>> <<Last Name>>

<<Address>>

<<City>>, TX. <<Zip>>

Dear <<Title>> <<Last Name>>:

Your name and certain personal information was [exposure type/description]. This means that information may have been exposed without your authorization or the authorization of [Agency]. We apologize for any inconvenience this offers you. [Although there is no evidence that any information has been misused, the state is providing you with free credit monitoring coverage.]

[Describe the incident and what the agency is doing to mitigate the incident.]

We are committed to helping you safeguard your information. [[Agency] is providing you with free credit monitoring and identity theft services for one year. This service includes an insurance policy of up to $[_] in identity theft coverage, a year of [name of Agency's contracted Breach Management Vendor product] coverage, and a full-service identity restoration team to guide you through the recovery process if anyone tries to misuse your information. You must enroll to take advantage of this free service.]

We have set up a website that will help you protect your information and will provide you with updates on this matter. You may also call [name of Agency's contracted Breach Management Vendor] to ask for help in keeping your data safe. **If you are enrolling a minor child, you will need to call [Breach Management Vendor] to process their enrollment manually. Child enrollment cannot be conducted online.**

We recommend that you also take the following steps to protect your identity:

- Contact one of the national credit reporting agencies below and ask for a fraud alert on your credit report. The agency will alert all other agencies. Remember to renew these fraud alerts every 90 days. The state does not have authority to do this for you, as the credit bureaus must have your permission to set up the alerts.
- The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You may contact each agency to determine if a child has a file or if the child's information has been misused:

Equifax
P.O. Box 740241
Atlanta, GA 30374

www.fraudalerts.equifax.com
Fraud Hotline (toll-free): 1-877-478-7625

Experian
P.O. Box 2002
Allen, TX 75013

www.experian.com
Fraud Hotline (toll-free): 1-888-397-3742

TransUnion
P.O. Box 6790
Fullerton, CA 92834

www.transunion.com
Fraud Hotline (toll-free): 1-800-680-7289
Report fraud: fvad@transunion.com

- Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.
- Monitor your [bank account activity / health care records / medical insurance company explanation of benefits] to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to your [bank / health care provider / health insurance company's privacy officer].
- Report any suspicious activities on your [credit reports or bank account / health care or health insurance records] to your local police or sheriff's office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.
- Learn about the Federal Trade Commission's identity theft programs by visiting www.ftc.gov/bcp/edu/microsites/idtheft or by contacting the Federal Trade Commission's toll-free Identity Theft helpline at 1-877-ID-THEFT (1-877-438-4339); TTY:1-866-653-4261.
- [Enroll in free credit monitoring and identity theft services provided by the state. There is no cost to you for the service, but **you must enroll**. You can enroll online at_____or by contacting [Agency's contracted Breach Management Vendor's] Customer Care Center toll-free at_____.]
- **[To enroll your minor child, please call [Agency's contracted Breach Management Vendor's] Customer Care Center at_____to manually enroll them. Child enrollments cannot be conducted online.]**
- Monitor the website at [Agency's contracted Breach Management Vendor's agency / Agency's own site] for periodic updates.

[Agency] regrets that this action is necessary. Please be assured that we are committed to helping you protect your credit and identity and in ensuring that your information is safe and secure.

If you have any questions, please call [Agency contact] at_____or contact by email at _____.

Sincerely,

[Authorized signatory]

8.4 Public (Media) Notice

In the event that you choose to notify the public at large, the information in your notice should mirror the information contained in the breach notice to individuals affected (section 7.3). Media notice may be legally required; please see Breach Notice Criteria. A media notice should be developed through your usual public communication processes and contain the following information:

- Brief description of the details of the event
- Description of the individuals affected in the aggregate
- Description of actions taken by the agency
- Statement as to whether evidence indicates the data may have been misused
- Contact information for questions

8.5 Post-Mortem and Improvement Plan

INCIDENT POST-MORTEM

Cyber Incident	[Use your organization's naming convention of the incident.]
Dates and Times	[Indicate at a minimum the start/end dates/times of the incident. Include a full incident chronology if available.]
Description	[Give a brief description of the incident.]
Impact	[What was the impact to the organization?]
Detection	[How was the incident detected?]

Learning and Improving

Question	Response	Comment
How well did the staff and management perform?	.	.
Were documented policy and procedures followed?	.	.
Were the procedures adequate?	.	.
Was the actual cause identified?	.	.
What information was needed sooner?	.	.
Were any steps taken that might have inhibited recovery?	.	.
What should/would staff/management do differently the next time a similar incident happens?	.	.
How could information sharing (in/out) with other organizations have been improved?	.	.
What corrective actions can prevent or lower the likelihood of similar incidents in the future?	.	.
What precursors or indicators of compromise should be watched in the	.	.

	future to speed up detection?		
	What additional tools and/or resources are needed to address future incidents?	.	.
	What tools, processes, metrics or resources could be in place and/or monitored to detect a similar incident sooner?	.	.

Root Cause Analysis

Question	**Response**	**Comment**
What could have prevented the incident?	.	.
Was there damage caused prior to detection?	.	.
Is the incident a recurrence of a previous incident?	.	.
Was the actual cause identified?	.	.
Was there a difference between initial impact assessment and the final impact assessment?	.	.
Were there any leading-edge indicators of detection that were missed?	.	.

Metrics	[Enter any related metrics e.g., mean-time-to-incident-discovery, cost of recovery, time from detection to containment, …]
Approximate cost of the incident	[What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, agency downtime, idle employee time, backlog catchup overtime, etc.]

IMPROVEMENT PLAN

This improvement plan has been developed specifically for [Organization] as a result of the Cyber Incident that occurred on [date].

Issue/Area for Improvement	Corrective Action	Primary Responsible	Start Date	Completion Date
1. [Area for Improvement]	[Corrective Action 1]			
	[Corrective Action 2]			
	[Corrective Action 3]			
2. [Area for Improvement]	[Corrective Action 1]			
	[Corrective Action 2]			

SECTION 9

External Contacts

External Partners. Collaboration with external entities may be necessary to assist with incident response or for auxiliary support. The IRT shall ensure that all those participating in the incident response work together efficiently and effectively.

The tables below identify contact information of external partners with whom the agency may need to collaborate in the event of an Incident as well as resource pages and other useful information.

Table 9.1: State of Texas Contacts

Resource	Services	Contact Information
Austin Police Department Digital Analysis Response Team (DART)	Conducts investigations of technology-related crimes in the City of Austin and helps other law enforcement agencies perform forensic examinations of digital evidence.	Contact number: (512) 974-8631
Office of the Attorney General	The agency of the state's chief law enforcement official.	OAG main number: (512) 463-2191 Deputy Attorney General for Defense Litigation: (512) 463-0150 State Law Enforcement Criminal Investigation: (512) 936-2777 Contact OAG Information Security Officer (for Incidents affecting OAG data system or staff). Identity Theft Legal Resources and Alerts: https://www.oag.state.tx.us/consumer/index.shtml
Office of the Attorney General, Criminal Investigations Division	Investigates cybercrime and provides computer forensics services to locate and preserve digital evidence.	Criminal Investigations: CJID@oag.state.tx.us (512) 475-4220 Cybercrimes: (512) 463-9570

State Auditor's Office, Special Investigations Unit	Investigates criminal offenses affecting state resources, including computer security breaches.	Hotline: 1-800-892-8348
Texas Facilities Commission	Provides facilities services (including emergency management) for state buildings and leasing services to state agencies.	24-hour Facilities Management: (512-) 463-3600 State Leasing Services: leasing@tfc.state.tx.us (512) 463-3331
Texas Department of Information Resources, Security Operations Center	Provides information security services and communications technology services, including Incident response and assistance, to Texas state agencies, local governments, public education entities, and special districts.	DIR Network Security Operations Center: Security-alerts@dir.texas.gov 888-839-6762 Option 1 network Option 2 Security
Texas Department of Public Safety, Emergency Management Division	Coordinates the state emergency management program and manages the Statewide Operations Center (SOC), which monitors threats, makes notification of threats, and provides information on emergency incidents to local, state, and federal officials.	Division of Emergency Management Headquarters: (512) 424-2138 SOC: soc@dps.texas.gov Operations Officers: (512) 424-2208 (512) 424-2277
Texas Rangers, Texas Department of Public Safety	Leads criminal investigative responsibility for major Incident crime investigations.	Austin Headquarters: (512) 424-2160 rangers@dps.texas.gov

Table 9.2: Federal Contacts

Resource	Services	Contact Information
Federal Bureau of Investigation	Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information.	Texas Field Offices: Dallas: (972) 559-5000 El Paso: (915) 832-5000 Houston: (713) 693-5000 San Antonio: (210) 225-6741
Federal Emergency Management Agency (FEMA)	Provides disaster response and recovery assistance.	1-800-621-FEMA (3362)
National Cyber Security Division (NCSD), US Dept. of Homeland Security	Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.	Response coordination: (202) 282-8000

CERT Coordination Center (CERT/CC)	Federally-funded CERT provide technical advice to federal, state, and local agencies on responses to security compromises.	CERT 24-hour hotline: (412) 268-7090 forensics@cert.org
US Secret Service	Investigates financial crimes, including identity theft.	Austin Field Office: (512) 916-5103
US Treasury Inspector General for Tax Administration (TIGTA) and Office of Safeguards	Works with agencies to ensure that all appropriate actions are taken with regard to Federal Tax Information.	TIGTA Field Division, Dallas: (972) 308-1400
Federal Trade Commission (FTC)	Regulates consumer business practices.	http://www.ftc.gov Detecting identity theft: http://www.ftc.gov/idtheft
National Institute of Standards and Technology (NIST), US Dept. of Commerce	Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 (FISMA, 44 USC § 3541, *et seq.*). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government.	Main office: (301) 975-NIST inquiries@NIST.gov http://www.nist.gov/index.html Publications: http://csrc.nist.gov/publications/
Office for Civil Rights (OCR), US Dept. of Health and Human Services	Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA.	http://www.hhs.gov/ocr/office/index.html
US Postal Service Inspector Service	The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees.	https://postalinspectors.uspis.gov

Table 9.3: Industry Contacts

Resource	Services	Contact Information
Ponemon Institute	Conducts independent research on privacy, data protection, and information security policy.	http://www.ponemon.org/index.php

Credit Bureaus	Collects reported consumer credit for purposes of credit risk assessment and scoring or other lawful purposes. Consumers may request a 90-day or 7-year fraud alerts be attached to their credit bureau files by contacting one credit bureau which will in turn notify other bureaus. A credit freeze must be requested from each bureau.	Equifax: P.O. Box 740241 Atlanta, GA 30374 Fraud Hotline (toll-free): 1-877-478-7625 www.fraudalerts.equifax.com Experian P.O. Box 2002 Allen, TX 75013 Fraud Hotline (toll-free): 1-888-397-3742 www.experian.com TransUnion P.O. Box 6790 Fullerton, CA 92834 Fraud Hotline (toll-free): 1-800-680-7289 www.transunion.com Email to report suspected fraud: fvad@transunion.com Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281 1-877-322-8228 http://www.ftc.gov/freereports www.AnnualCreditReport.com
American Health Information Management Association (AHIMA)	AHIMA is an association of health information management professionals with a useful resources page for health data.	http://www.ahima.org/resources/infocenter/psc.aspx
Health Information Management Systems Society (HIMSS)	HIMSS is an association of health information management professionals with resources page for health data.	http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=17266
Payment Card Industry – Data Security Standards (PCI-DSS)	Payment card data security standards set by the payment card industry.	https://www.pcisecuritystandards.org/security_standards/

Table 9.4: Press Contacts

Resource	Services	Contact Information
Texas Press Contacts	Texas Media Directory (subscription for distribution lists for other cities and counties).	http://www.texasmedia.com

SECTION 10

Legal References

This section covers a list of federal and state laws establishing relevant standards for types of confidential data, including a brief summary and a citation. The list is not comprehensive; please refer to legal counsel for other relevant laws.

10.1 Texas Laws and Regulations for Data Privacy and Security

Texas Public Information Act

The Public Information Act contains provisions pertaining to information disclosure:

The agency may not withhold information, even confidential information, if requested by a legislator or the Legislature for legislative purposes.	TGC § 552.008
Information confidential by law is excepted from disclosure. Example: TGC § 2059.055.	TGC § 552.101

Is this IRT Redbook subject to disclosure under the Public Information Act? Some possible exceptions to disclosure for all or part of the book:

Employee home addresses, home phone numbers, social security numbers, and family information is exempted from disclosure if the employee did not choose to disclose under §522.024, which may apply to IRT contact information. Note: employee home email addresses possibly also excepted under 552.117. Unresolved issue: disclosure of employee work email address (otherwise public) may reveal who is on IRT.	TGC § 552.117
Network security is exempted from the requirement to disclose in the Public Information Act.	TGC § 552.139, TGC § 2054.055, ORD 581 (1990)

Are records relating to the breach itself and the agency's response confidential? Possible exceptions to disclosure include:

Some personnel information may be private if in the personnel file; some transcripts are exempt from disclosure.	TGC § 552.102, TGC § 552.024, TGC § 552.117
Information related to litigation, if pending or reasonably anticipated, is exempt from disclosure.	TGC § 552.103
Information related to competition or bidding, generally while bidding is in process, is exempt from disclosure.	TGC § 552.104, TGC § 552.128

	Information submitted by a potential vendor or contractor is also exempted from disclosure.	
	Attorney-client privilege and court-ordered confidentiality can be used to keep certain information from disclosure, with some limitations (see TGC § 552.022(b)).	TGC § 552.107, TGC § 552.022(b)
	Certain law enforcement records may be kept private, generally while the case is pending.	TGC § 552.108
	Trade secrets are exempt from public disclosure.	TGC § 552.110
	Agency memoranda which would not be made available to a party in litigation (including attorney work product) are exempt from disclosure.	TGC § 552.111
	Credit and debit card numbers as well as access device numbers may be kept from disclosure; additionally according to ORD 684 (2009), insurance policy numbers, bank account numbers, and bank routing numbers can also be withheld from disclosure.	TGC § 552.136, ORD 684 (2009)
	Email addresses of the public are exempt from disclosure.	TGC § 552.137
	Social security numbers are exempt from disclosure.	TGC § 552.147
	Note: the information that was the subject of the breach is also presumed to be protected from disclosure, possibly under sections not cited above. Each agency should be aware of how its own information is protected under the Public Information Act.	
	With a few exceptions, agencies must receive a decision from the Office of the Attorney General before it can withhold information from a PIA request. The PIA contains some pitfalls, including some very strict deadlines. All agencies should consult an attorney or PIA coordinator for further guidance.	
Privacy Policy Necessary to Require Disclosure of SSN	A person may not require an individual to disclose one's social security number to obtain goods or services from or enter into a business transaction with the person unless the person adopts a privacy policy, makes the policy available to the individual, and maintains the confidentiality and security of the social security number. The statute also prescribes required elements of a privacy policy.	BCC § 501.052
Texas Identity Theft Enforcement and Protection Act	The Texas Identity Theft Enforcement and Protection Act requires notification to customers in the event of a security breach of customer's computerized data, specifically customer's personally identifiable information (PII). The	BCC Ch. 521

	notification must be done as quickly as possible. The Act does provide for remedies not to exceed $50,000 per violation. If more than 10,000 individuals were affected by a breach, consumer reporting agencies must be notified. The Act does have a safe harbor when data is protected with encryption.	
Texas Medical Records Privacy Act	The Texas Medical Records Privacy Act is Texas law making Protected Health Information confidential. This law is applicable to "Texas covered entities" or "any person who… comes into possession of protected health information," a term more broadly defined than HIPAA's "Covered Entities" and "Business Associates" (collectively: healthcare providers, healthcare clearing houses, health plans, and any business associates of the aforementioned).	HSC Ch. 181
Texas Administrative Code	Information Security Standards for State Agencies and Institutions of Higher Education.	1 TAC 202
	Administrative rule pertaining to agencies' websites.	1 TAC 206
	Each agency and institution of higher education must protect the privacy and personal identifying information (PII) of a member of public who provide or receive information from or through the institution's website. Prior to providing access to information or services on a state website that requires PII, each institute must conduct a transaction risk assessment and implement appropriate safeguards that conform to TAC 202.	1 TAC § 206.52, 1 TAC § 206.72
	Texas rule in line with HIPAA, Privacy of Health Information, etc.: provides for the privacy of health information, an individual's right to correct such information, and the process for doing so.	25 TAC § 1(W)

10.2 Federal Laws and Regulations for Data Privacy and Security

Health Insurance Portability and Accountability Act (HIPAA) (1996)	HIPAA contains the following provisions regulating the use and disclosure of protected health information: • *Privacy Rule* protects the privacy of individually identifiable health information; • *Security Rule* sets national standards for the security of electronic protected health information;	HIPAA (1996);

	• *Breach Notification Rule* requires covered entities and business associates to provide notification following a breach of unsecured protected health information; • *Enforcement* providing civil and criminal penalties for violation; and • *Patient Safety Rule* protects identifiable information being used to analyze patient safety events and improve patient safety.	
Health Information Technology for Economic and Clinical Health Act (HITECH) (2009)	HITECH amended HIPAA in 2009 with interim regulations, expanding direct liability to HIPAA Business Associates and requiring Covered Entities and Business Associates to report data breaches to those affected individuals through specific breach notification requirements.	HITECH (2009) (ARRA Title XIII)
HIPAA Omnibus Regulations (2013)	These regulations made substantial changes to HIPAA: • The Omnibus Regulations finalized the interim HITECH regulations; • Made Business Associates directly liable for certain Privacy and Security requirements; • Enacted stronger prohibitions on marketing (opt-out) and sale of Protected Health Information (PHI) without authorization; • Expanded individuals' rights to receive electronic copies of PHI; • Allowed individuals the right to restrict disclosures to a health plan concerning treatment for which the individual has paid out-of-pocket in full; • Required Notice of Privacy Practices updates and redistribution; • Changed authorization related to research and disclosure of school proof of child immunization and access to decedent information by family members or others; • Enhanced enforcement in many ways, including addressing the enforcement against noncompliance with HIPAA Rules due to willful neglect; • Finalized the rule adopting changes to the HIPAA Enforcement Rule to incorporate tiered, mandatory penalties up to $1.5 million per violation; and • Finalized rule adopting GINA and prohibited most health plans from using or disclosing genetic information for underwriting purposes, as proposed in Oct. 2009.	45 CFR Parts 160-164
Family Educational Rights and	FERPA creates a right of privacy regarding grades, enrollment, and billing information. Specifically, this information may not be released without prior consent	20 USC § 1232G; 34 CFR Part 99

Privacy Act (FERPA) (1974)	from the student. In addition to safeguarding individual student records, the law also governs how state agencies transmit testing data to federal agencies.	
Federal Information Security Management Act (FISMA) (2006)	Federal legislation that assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to provide for the strengthening of information security systems. Specifically, the Act requires heads of each agency to implement policies and procedures to effectively and efficiently drive down IT security issues to acceptable levels through a defined framework by which federal government agencies would ensure the security of information systems controlled by either the agency or one of its contractors on behalf of a federal agency. The framework is further defined by the standards and guidelines set forth by NIST.	44 USC §§ 3541-3549
Internal Revenue Service Statute and Regulation	Through Publication 1075, the IRS has created a framework by which Federal Tax Information (FTI) and Personally Identifiable Information (PII) is protected from public disclosure. To ensure the safety of such data, receiving agencies and/or entities must have proper safeguards in place. Federal code requires external agencies and other authorize recipients of federal tax return and return information (FTI) to establish specific procedures to ensure the adequate protection of the FTI they receive. In addition, the same section of the Code authorizes the IRS to suspend or terminate FTI disclosure to a receiving agency or other authorized recipient if misuse or insufficient FTI safeguards are found. In addition to criminal sanctions, the Internal Revenue Code prescribes civil damages for unauthorized disclosure and, when appropriate, the notification to affected taxpayers that an unauthorized inspection or disclosure has occurred.	Publication 1075; IRC Section 6103(p)(4); 26 USC §6103(p)(4)
Social Security Administration (SSA) Statute and Regulation	Much of the information SSA collects and maintains on individuals is especially sensitive, therefore prior to disclosing of such information, SSA must look to the Privacy Act of 1974, 5 USC Section 552a, FOIA, 5 USC Section 1106 of SSA, 42 USC Section 1306. SSA employees are prohibited from disclosing any information contained in SSA records unless disclosure is authorized by regulation or otherwise required by federal law. SSA may only disclose personal records (PII) when the individual to whom the record pertains provides written consent or when such disclosure falls into one of the several narrowly-drawn exceptions.	Privacy Act of 1974; 5 USC Section 552a; FOIA; 5 USC §1106 (SSA); 42 USC §1306

National Institute of Standards and Technology (NIST)	NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and to help with managing cost effective programs to protect their information systems and the data stored on the systems. NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in FIPS 200. The security rule covers 17 areas, including control, incident response, business continuity, and disaster recoverability. A key part of the certification and accreditation process for federal information systems is selecting and implementing a subset of the controls. Agencies are expected to comply with NIST security standards and guidelines.	NIST 800-53 rev. 4; FIPS 200
Criminal Justice Information Services (CJIS)	CJIS is a division of the FBI that compiles data provided by law enforcement agencies across the United States. CJIS is the world's largest repository of criminal fingerprints and history records which can be accessed and searched by law enforcement to enable the quick apprehension of criminals. The responsibility of CJIS extends to the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Incident-Based Reporting System (NIBRS). In addition to its many responsibilities in the coordination and sharing of criminal data, CJIS promulgates the CJIS Security Policy, which is meant to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI). The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI data. The policy applies to every individual – contractor, private entity, noncriminal justice agency representatives, or members of a criminal justice entity – with access to, or who operate in support of, criminal justice services and information.	CJIS Security Policy, TGC § 552.108
Clinical Laboratory Improvements Amendments (CLIA)	CLIA are federal regulatory standards applying to clinical laboratory testing performed on humans in the United States. The CLIA Program sets standards and issues certificates for clinical laboratories. The objective of CLIA is to ensure the accuracy, reliability, and timeliness of test results regardless of where the test is performed. All clinical laboratories must be properly certified to receive Medicare and Medicaid payments. The primary responsibility for the administration of this program is held by the Centers for Medicare and Medicaid Services.	CLIA Regulations and Guidance

Computer Fraud and Abuse Act (CFAA)	CFAA is a federal law passed to address computer-related crimes. The Act governs cases with a compelling federal interest; where computers of the federal government or certain financial institutions are involved; where the crime is interstate in nature; or where computers are used in interstate and foreign commerce. The CFAA defines "protected computers" as those exclusively used by financial institutions or the US Government, or when the conduct constituting the offense affects the use by or for the financial institution or the federal government, or those computers which are used in or affecting interstate or foreign commerce or communication.	18 USC §1030

10.3 Other Laws and Regulations for Data Privacy and Security

General Data Protection Regulation (GDPR) (2018)	The General Data Protection Regulation (GDPR) is a privacy and security law drafted and passed by the European Union (EU). It imposes obligations onto organizations across the globe, so long as they target or collect data related to people in the EU. The GDRP includes many key regulatory points, including: • Data protection principles • Accountability • Data security • Data protection by design and by default • When you're allowed to process data • Consent • Data Protection Officers • Privacy rights	GDPR (2018)

Acknowledgements

Version 1 of the Incident Response Form was published on behalf of the Department of Information Resources, with the input of the Statewide Information Security Advisory Committee, Privacy Advisory Committee, Data Breach Response Subcommittee. The members included:

Co-Chair: Sheila Stine, JD, Health and Human Services Commission, Chief Privacy Officer

Co-Chair: Martin Zelinsky, JD, Department of Information Resources, General Counsel

Chad Lersch, JD, Department of Information Resources, Assistant General Counsel

Betsy Loar, JD, Credit Union Department, Assistant Commissioner and General Counsel

Shelley Janda, JD, Department of Aging and Disability Services, Assistant General Counsel

Susan Maldonado, JD, Texas Facilities Commission, Assistant General Counsel

Their participation in creating this document is appreciated.

The current version of this document is maintained by the Department of Information Resources, Chief Information Security Office.

APPENDIX F

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

PREPARE

What is Ransomware:

Ransomware is a type of malicious software (malware), which denies access to systems or data and/or exfiltrates data.

How Ransomware Works:

Typically, the malware displays an on-screen alert advising the victim that their device is locked or their files are encrypted. In some cases, after an initial infection, ransomware attempts to spread to connected devices and systems.

Characteristics:

Non-encrypting ransomware locks the screen and restricts access to files.

Encrypting ransomware prevents computers from being booted up in a live environment by encrypting the Master Boot Record (MBR).

Leakage or "extortionware" exfiltrates data.

Mobile device ransomware infects cellphones through drive-by downloads or fake apps.

How Ransomware is Used:

Cyber actors hold systems or data hostage until a ransom is paid for a decryption key. Cyber actors also threaten to publish exfiltrated data, or sell it on the dark web. Increasingly, cyber actors request virtual currency transfers as a ransom payment method.

Incident Response (IR) Planning:

The U.S. Secret Service developed a Preparing for a Cyber Incident - Introductory Guide, which describes what actions organizations should take to cultivate an understanding of the technological and regulatory limitations, responsibilities, and resources available to them, and how to apply the acquired knowledge to their operations.

Paying Ransom Demand:

Paying the ransom does not guarantee regaining access. In some cases, a decryption key was not provided in return to a paid ransom. In other cases additional ransom was demanded.

Contacting Law Enforcement:

Reach out to law enforcement before contacting the cyber actor. Include law enforcement in your response plan. Contact the local U.S. Secret Service Cyber Fraud Task Force.

United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

PREVENT

Patches	Update operating systems, software, and firmware on devices with the latest patches. Consider using a centralized patch management system.
User Permissions	Restrict user permissions for installing and running software applications. Apply the principle of least privilege to all systems and services.
Email Scanning	Scan all incoming and outgoing emails to detect and filter threats, such as phishing and spoofing emails, and executable files (used to perform various functions or operations on devices). This will prevent them from reaching end users.
Firewalls	Configure your firewalls to block access to known malicious IP addresses.
Application Whitelisting	Use application whitelisting to reduce the risk of execution of malware, and unlicensed and unauthorized software. An application whitelist is a list of applications and application components that are authorized to execute on a host.
Awareness	Implement a training and awareness program for all employees.
Controls	Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations (temporary folders supporting popular Internet browsers, compression/ decompression programs).
Remote Access	Consider disabling Remote Desktop Protocol (RDP) if it is not being used.
Virtualization and Separation	Execute operating system environments or specific programs in a virtualized environment (multiple simulated environments). Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.
Backups	Have cold storage backups and test restoration of backup files regularly. This prevents the ransomware from infecting network-connected backup files.

United States Secret Service
Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

A GUIDE TO RANSOMWARE

RESPOND

A. Do not power down or shutoff any systems affected by ransomware.

B. Isolate the infected device and the compromised portion of your network as soon as possible.

C. Secure backups by taking them offline and ensure they are free of malware.

D. Use out-of-band methods of communication, and do not trust the entire network system.

E. Collect and secure partial portions of the ransomed data that might exist.

F. Collect all available log information.

G. Change online account and network passwords after removing the system from the network.

H. Use the oldest back-up to restore the system, if you have multiple backups.

IDENTIFY AND RECORD THE FOLLOWING INFORMATION:

- ✓Ransomware variant name.
- ✓What systems are affected.
- ✓Original emails with full headers and any attachments, if attack was executed by phishing.
- ✓Copies of executables or other files dropped onto the system after accessing malicious attachments, including a splash page.
- ✓Any domains or IP addresses communicated with just prior to or during infection.
- ✓Virtual currency addresses to which payment is requested, and the amount being requested.
- ✓Any forensic analysis or incident response reports completed.
- ✓Any memory captures taken during execution of the malware.
- ✓Status of the infection.
- ✓Provide network topology.

Contact the local U.S. Secret Service
Cyber Fraud Task Force Network Intrusion Team

APPENDIX G

RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Overview

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

This *Ransomware Guide* includes two resources:
Part 1: Ransomware Prevention Best Practices
Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): **https://learn.cisecurity.org/ms-isac-registration**
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): **https://learn.cisecurity.org/ei-isac-registration**
  - Sector-based ISACs - National Council of ISACs: **https://www.nationalisacs.org/member-isacs**
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: **https://www.isao.org/information-sharing-groups/**
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more.
  - SLTT organizations: **CyberLiaison_SLTT@cisa.dhs.gov**
  - Private sector organizations: **CyberLiaison_Industry@cisa.dhs.gov**

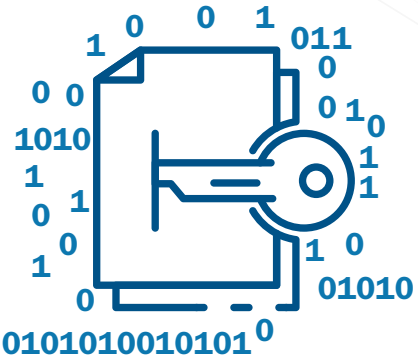
Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.



Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (**https://us-cert.cisa.gov/ncas/alerts/aa20-073a**).
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:
  - Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.
    - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
  - Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both "precursor" malware and ransomware.
  - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
  - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
  - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
  - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.

For more information on DMARC, see: **https://www.cisecurity.org/blog/how-dmarc-advances-email-security/** and

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf.

Funded by CISA, the MS-ISAC and EI-ISAC provide the Malicious Domain Blocking and Reporting (MDBR) service at no-cost to members. MDBR is a fully managed proactive security service that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known malware, ransomware, phishing, and other cyber threats. To sign up for MDBR, visit: **https://www.cisecurity.org/ms-isac/services/mdbr/.**

CISA and MS-ISAC encourage SLTT organizations to consider the Albert IDS to enhance a defense-in-depth strategy. CISA funds Albert sensors deployed by the MS-ISAC, and we encourage SLTT governments to make use of them. Albert serves as an early warning capability for the Nation's SLTT governments and supports the nationwide cybersecurity situational awareness of CISA and the Federal Government. For more information regarding Albert, see: **https://www.cisecurity.org/services/albert-network-monitoring/.**

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
  - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers (**https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers**).
  - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
  - Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
  - If you are using passwords, use strong passwords (**https://us-cert.cisa.gov/ncas/tips/ST04-002**) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
  - Restrict user permissions to install and run software applications.
  - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.

- Remove unnecessary accounts and groups and restrict root access.
- Control and limit local administration.
- Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
- Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.

- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (**https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a**).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
  - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.

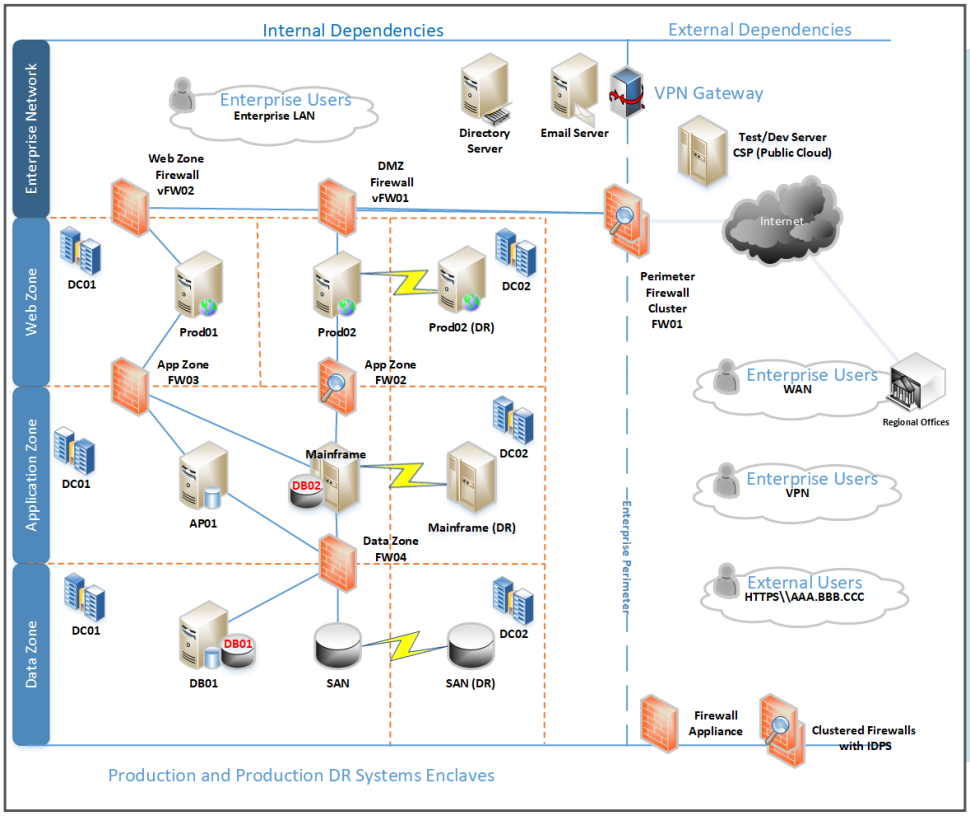


Figure 1. Example Network Diagram

This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.

- Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: **https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/**.

- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).

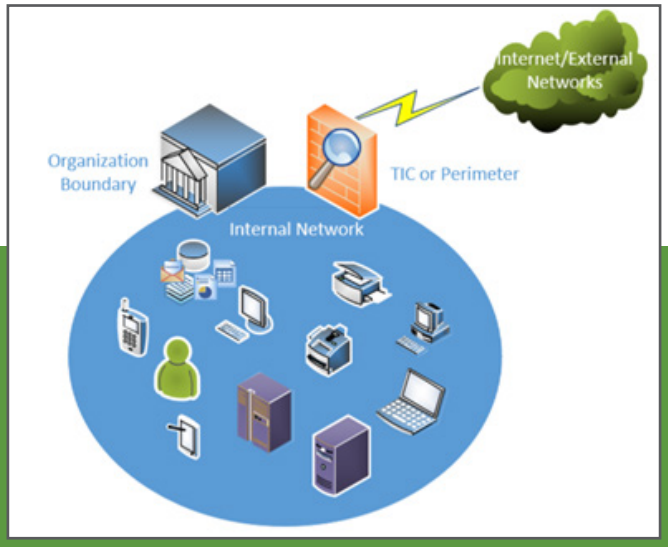


Figure 2. Flat (Unsegmented) Network

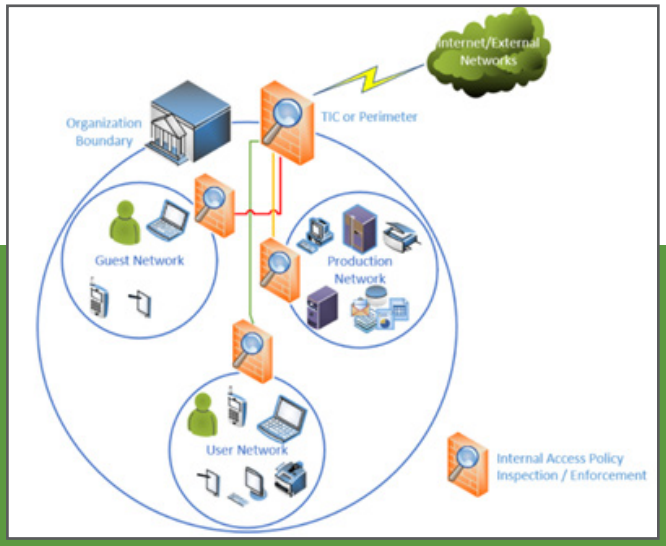


Figure 3. Segmented Network

- The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

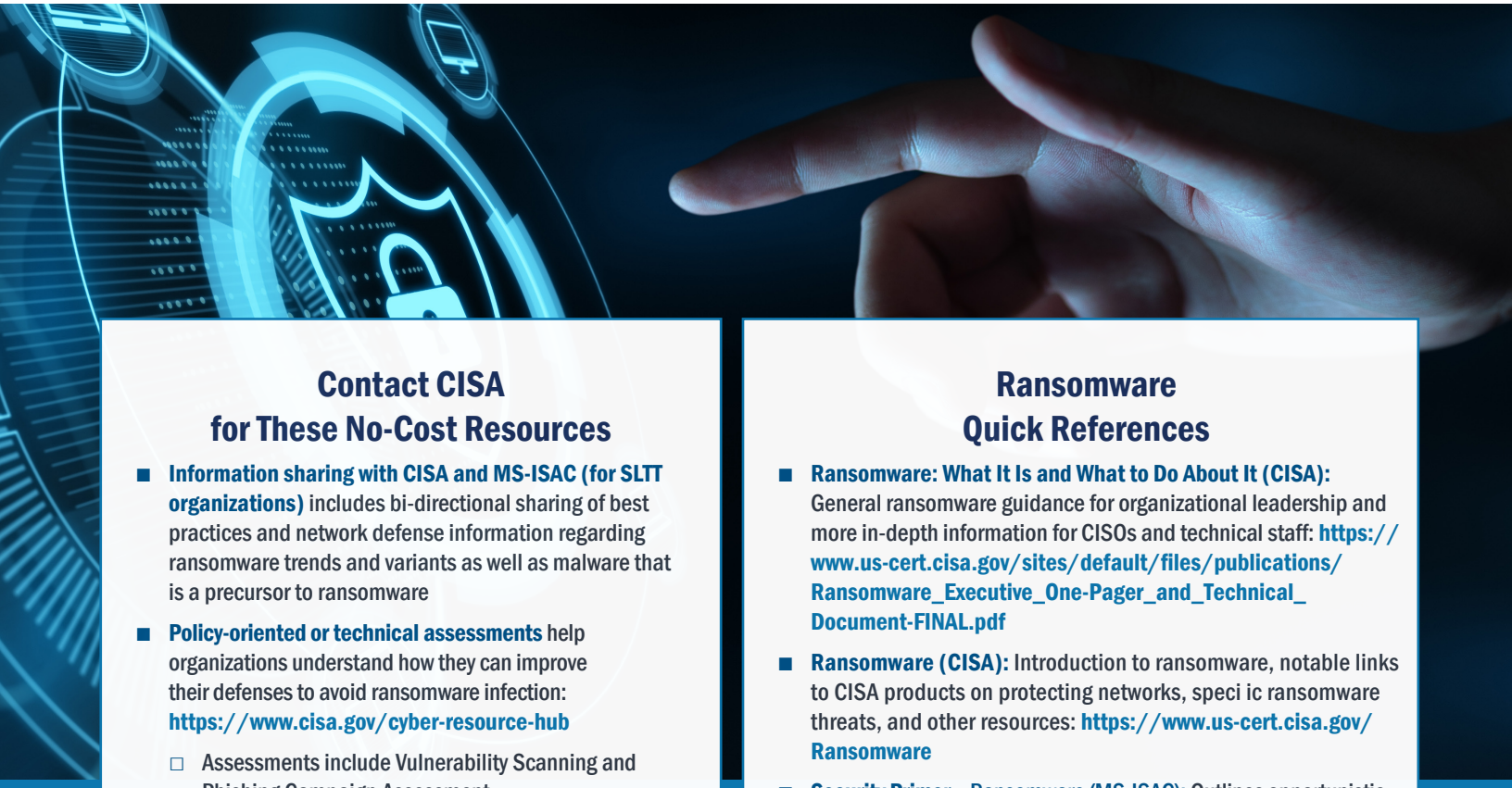
- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
  - The following list contains high-level suggestions on how best to secure a DC:
    - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
    - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory**), when configuring available security features.
    - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
    - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
    - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
  - CISA recommends the following DC Group Policy settings:

    (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
    - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
    - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
    - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.

- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.

- Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.



Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: **https://www.cisa.gov/cyber-resource-hub**
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
  - **SLTT organizations:** **CyberLiaison_SLTT@cisa.dhs.gov**
  - **Private sector organizations:** **CyberLiaison_Industry@cisa.dhs.gov**

Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: **https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf**
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, speci ic ransomware threats, and other resources: **https://www.us-cert.cisa.gov/Ransomware**
- **Security Primer –** Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: **https://www.cisecurity.org/white-papers/security-primer-ransomware/**
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: **https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/**
- **Security Primer – Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: **https://www.cisecurity.org/white-papers/security-primer-ryuk/**

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

☐ **1. Determine which systems were impacted, and immediately isolate them.**

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ **2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.**

☐ **3. Triage impacted systems for restoration and recovery.**

- ☐ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
  - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ **4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

☐ **5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.**

- ☐ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- ☐ Recovered executable file
- ☐ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- ☐ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Malware samples
- ☐ Names of any other malware identified on your system
- ☐ Encrypted file samples
- ☐ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- ☐ Any PowerShell scripts found having executed on the systems
- ☐ Any user accounts created in Active Directory or machines added to the network during the exploitation
- ☐ Email addresses used by the attackers and any associated phishing emails
- ☐ A copy of the ransom note
- ☐ Ransom amount and whether or not the ransom was paid
- ☐ Bitcoin wallets used by the attackers
- ☐ Bitcoin wallets used to pay the ransom (if applicable)
- ☐ Copies of any communications with attackers

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.

- ☐ Consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS]). See contact information below.
- ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
- ☐ The *Public Power Cyber Incident Response Playbook* (https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf) contains guidance for organizational communication procedures as well as templates for cyber incident holding statements for public consumption. Work with your team to develop similar procedures and draft holding statements as soon as possible, as developing this documentation during an incident is not optimal. This will allow your organization to reach consensus, in advance, on what level of detail is appropriate to share within the organization and with the public, and how information will flow.

Containment and Eradication

If no initial mitigation actions appear possible:

☐ 6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.

- ☐ Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

☐ 7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

To continue taking steps to contain and mitigate the incident:

☐ 8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

- ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files.

☐ 9. Identify the systems and accounts involved in the initial breach. This can include email accounts.

☐ 10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:

- ☐ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ 11. Additional suggested actions—server-side data encryption quick-identification steps:

- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:

  1. Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.

  2. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

  3. Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.

  4. Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.

  5. Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., "smb2.filename contains cryptxxx").

☐ 12. Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested:

- CISA – Advanced Malware Analysis Center: **https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf**
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): **https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/**
  - ☐ Scans a suspicious file or Uniform Resource Locator (URL) against several antivirus vendors to determine if it matches known malicious signatures
  - ☐ Runs a file or URL in a sandbox to analyze behavior
  - ☐ Provides a user with a summary report of malware behavior, including files accessed, tasks created, outbound connections, and other behavioral traits
  - ☐ Users can opt to keep submissions private and make direct requests for assistance from MS-ISAC; users can also mark submissions for sharing with CISA
  - ☐ Email: **mcap@cisecurity.org** to set up an account
- Remote Assistance – Request via CISA Central or MS-ISAC Security Operations Center (see contact information below)

- ☐ Look for evidence of precursor "dropper" malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet.
  - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying.
  - Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

☐ 13. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.

- ☐ Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- ☐ Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- ☐ Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ 14. Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible.

☐ 15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

☐ 16. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.

Recovery and Post-Incident Activity

☐ 17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.

- ☐ Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.

☐ 18. Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

☐ 19. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community.

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- Contacts:
  - CISA:
    - **https://us-cert.cisa.gov/report**, **Central@cisa.gov** or (888) 282-0870
    - Cybersecurity Advisor (**https://www.cisa.gov/cisa-regions**): [Enter your local CISA CSA's phone number and email address.]
  - MS-ISAC:
    - **soc@msisac.org** or (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- Contacts:
  - FBI:
    - **https://www.fbi.gov/contact-us/field-offices**
    - [Enter your local FBI field office POC phone number and email address.]
  - USSS:
    - **https://www.secretservice.gov/contact/field-offices/**
    - [Enter your local USSS field office POC phone number and email address.]

DEFEND TODAY,
SECURE TOMORROW

CISA.GOV

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®