ALFA International
THE GLOBAL LEGAL NETWORK

2024 International Client Seminar

February 29 - March 3, 2024

Skeletons in the Closet: Navigating Privacy Issues for Better Data Protection and Brand Success in the Future

Nick Brauns
Moderator
HIGGS FLETCHER & MACK, LLP
San Diego, California
braunsn@higgslaw.com

Krystle Dalke
HINKLE LAW FIRM LLC
Wichita, Kansas
kdalke@hinklaw.com

The Case Study of Company ABC's Ransomware Event

Background on Company ABC

Company ABC is an oil and gas company with operations in several states within the United States. Company ABC has approximately two hundred employees. Company ABC owns and operates numerous oil and gas interests and has several affiliated businesses.

Company ABC employs the following security controls:

- Virtual servers on Nimble Systems (domain controllers, internally hosted email, print server, etc.);
- Dedicated backup systems (VEAAM, StoreOnce);
- Backup systems are both onsite and replicated offsite; and
- Backup data is read only, meaning it cannot be opened and corrupted.
- Company ABC does not have cyber liability coverage, but had engaged private cybersecurity experts to provide cybersecurity services, including penetration testing and security audits, prior to the ransomware event.

The Monday Morning Ransomware Event

Early Monday morning in late September 2021, an employee of Company ABC noticed that Company ABC's email server had stopped working and was not processing emails. This employee reported the email issue to Company ABC's IT department. Alarms did not immediately sound because Company ABC hosts its own email internally and it had experienced downtime before due to system updates and various other legitimate reasons. However, when the IT department attempted to log on to the email server, the administrator password did not work. Company ABC quickly discovered that the administrator credentials had been changed. Further investigation yielded a ransom note informing Company ABC that its servers and applicable data had been encrypted. The cybercriminals threatened disclosure of trade secrets and other sensitive data on the dark web. Company ABC did not take any chances and immediately took its systems offline to preserve any uncompromised data and prevent further corruption. Company ABC's IT department informed management of the ransomware attack. Company ABC's management and IT department communicated to all employees to power off all computers and devices inside the facility and connected field offices. Company ABC also contacted its cybersecurity expert consulting company to manage Company ABC's remediation process. Company ABC refused to pay the ransom and did not contact the cybercriminals.

The next 72 hours were a whirlwind for Company ABC. All IT department staff slept on site for three days. Additionally, Company ABC utilized a third-party forensic company to assist in recovery, which had two full-time employees on site for three days and other employees off and on during that same time. Efforts were spent:

1. Determining when the breach occurred, which was critical to determine the data recovery point. If the systems were recovered from a point after the breach, then the hacked access point and

ransomware virus would remain on the system.

2. Finding available backups that could be used for recovery of encrypted data. Company ABC's servers are virtual, so all servers (domain controllers, email, print servers, etc.) had to be recovered. Additionally, all shared file directories had to be recovered.
3. Once the recovery files were identified, all systems were recovered. The recovery process took over 24 hours to complete.

After the systems were recovered, Company ABC spent the next two days rebuilding every computer. All computers and devices connected to the system in the corporate office and field offices were wiped and reloaded from scratch or replaced with new hardware to ensure that the ransomware virus was no longer hiding on a local computer.

Because Company ABC's computers and systems were disconnected during the investigation and recovery process, Company ABC had to get creative to run payroll that Wednesday (two days after the initial ransomware event). Company ABC also had to pay several hundred invoices from its vendors. Luckily, Company ABC's legacy software for the oil and gas company resided on an IBM AS400 server that was not infected by the ransomware virus. Company ABC built a clean computer that plugged directly into the AS400 to create a dumb terminal. Company ABC also had one printer that was not corrupted by the ransomware attack because it was an IBM printer and did not run through the normal network. Company ABC's cybersecurity experts retrieved from a backup specific excel files and cleaned them for use. These adaptive actions enabled Company ABC to painstakingly bypass the normal network and run payroll and pay vendor invoices, allowing Company ABC to comply with its legal and contractual obligations owed to employees and vendors.

Ultimately, Company ABC only lost approximately four hours of work and was down for one week. After Company ABC recovered the lost data, it conducted an internal investigation into the ransomware event with the help of its cybersecurity service provider. Company ABC discovered that a Microsoft Exchange vulnerability announced on or around August 21, 2021, was the first weak link. Microsoft released a patch to fix the vulnerability, and Company ABC's consulting firm applied the patch around 3:30 p.m. that same day. Subsequent investigation revealed that the cybercriminals placed the ransomware file on Company ABC's email server at approximately 1:30 p.m., just two hours before Company ABC applied the patch. Neither Company ABC nor their general consultant checked logs and did not have protective software in place to inform Company ABC that this file had been placed on its email server, the second weak link. While it was not determined which employee allowed the access, it was determined that the only possible way for the access to be granted to the cybercriminals was through an email link that was clicked by an employee, the third weak link. Although social engineering ultimately allowed the breach, not Company ABC's firewalls and other security controls, there was a series of weak links that created the opportunity for the cyberattack to occur.

Once inside Company ABC's system, the cybercriminals waited approximately 30 days to ensure that the suspected standard backup protocols had been corrupted and Company ABC would be more inclined to pay the ransom because it lacked good backups. Company ABC believes that the cybercriminals were able to determine that Company ABC was in a vulnerable state because it was in the middle of replacing its backup systems. Company ABC had recently learned that its offsite backup systems were not

configured correctly when they were replaced in March 2021. Company ABC had ordered additional hardware to remedy the improper configuration and was awaiting delivery of this hardware at the time of the cyberattack. Company ABC believes the timing of the ransomware encryption was deliberate because the cybercriminals had sufficient time to learn about Company ABC's vulnerabilities.

Company ABC also learned that the cybercriminals had posted a small sub-set of Company ABC's files to the dark web after Company ABC did not pay the ransom. Fortunately, Company ABC's cybersecurity experts were able to identify what files had been posted and Company ABC was able to mitigate any damage caused by the leak on the dark web. Company ABC shut down two bank accounts. Through the assistance of legal counsel, Company ABC concluded that no notifications to regulators or impacted individuals were needed because only one executive's information was posted and that executive had already received notice and taken steps to protect impacted personal information. Additionally, the bulk of files posted were encrypted with Company ABC's applied passwords that had not been compromised.

While Company ABC had to scramble and spend its resources on cybersecurity experts and hardware to replace compromised computers and devices, Company ABC's ransomware attack was relatively small compared to other businesses. Company ABC was aware from contacts within the oil and gas industry that another oil and gas company had experienced three separate ransomware attacks within a one-year period. Each time the other oil and gas company paid the ransom to retrieve its encrypted files, only to have the same cybercriminals come back and ask for a higher ransom.

Following the post-breach investigation, Company ABC took steps to prevent a similar type of cyberattack by installing software that would identify any file loaded on its server, or attempted loading, and block it unless otherwise approved. Additionally, Company ABC hired an outside security company to monitor the logs. Company ABC also gave the outside security company authority to immediately shut down Company ABC's servers if another cyberattack is suspected.

A Closer Look at Ransomware

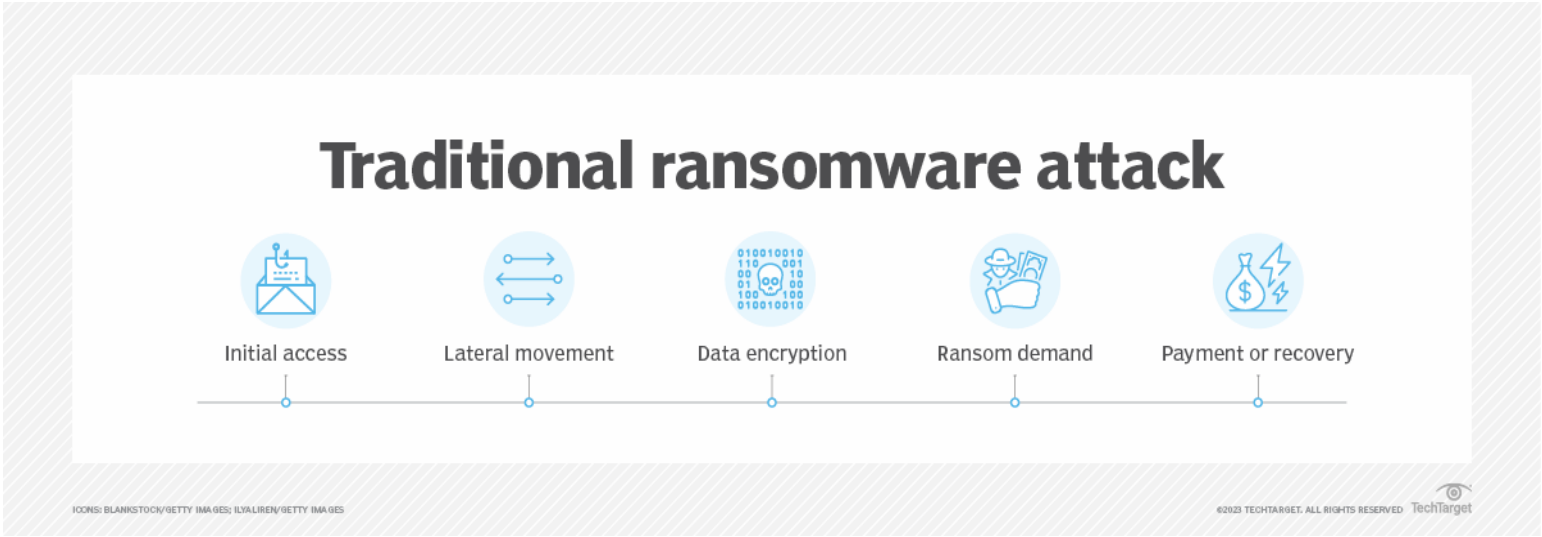
While the digital age is great for efficiency, opportunity, and brand presence, it also brings many cyber risks that are here to stay. Just like Company ABC, organizations must take action to guard against and mitigate these cyber risks.

What is Ransomware?

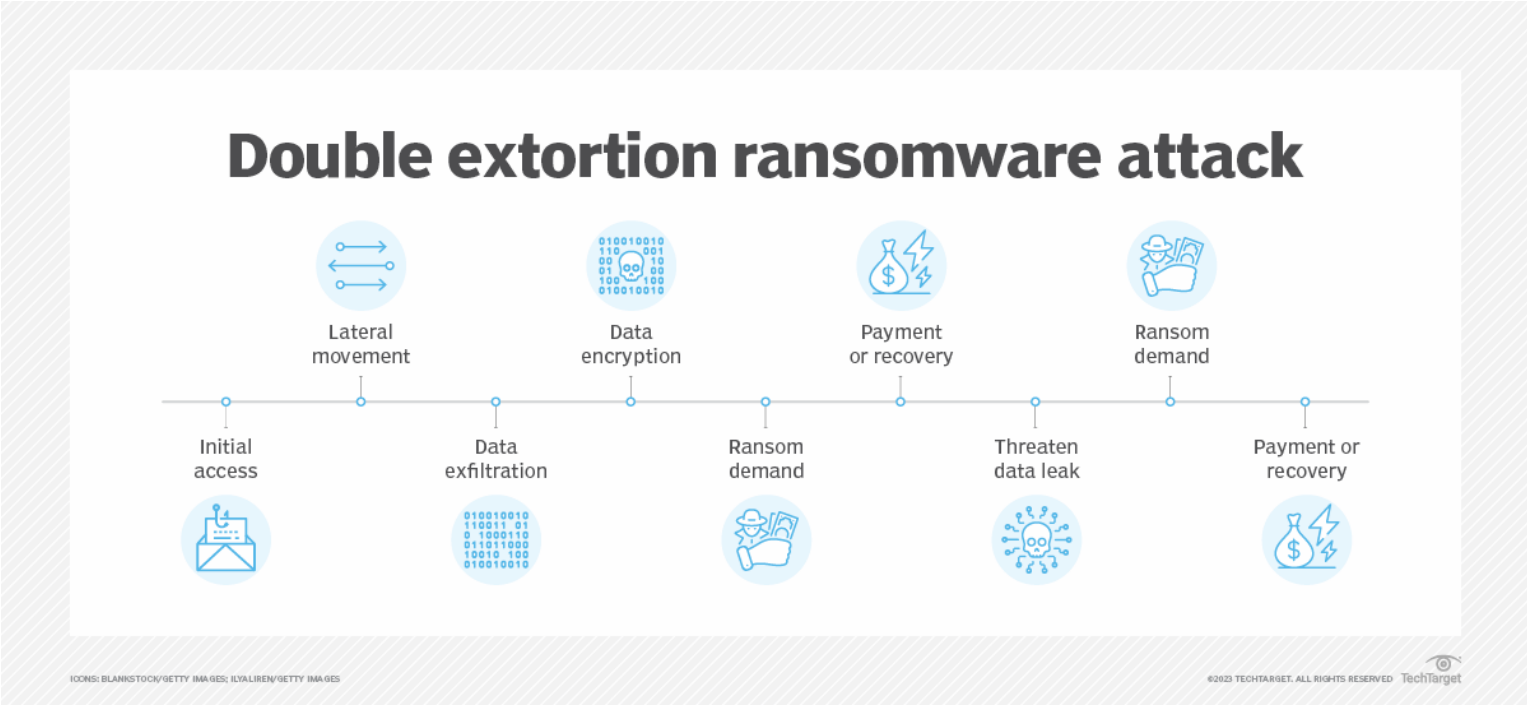
The National Cyber Investigative Joint Task Force ("NCIJTF") defines ransomware as "a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cybercriminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public."[i] Cybercriminals are often sophisticated and operate criminal enterprises just like any ordinary, legitimate business. The motivation behind a cybercriminal's attack varies, ranging anywhere from terrorism, financial gain, reputational damage, or access to confidential information or trade secrets. These cybercriminals are skilled at preying on a business's pain points and know where to push to get the most bang for their buck.

There are multiple types of ransomware attacks. Ordinary ransomware attacks result in encryption of data, preventing the business from accessing or using the data. Below is a diagram prepared by

TechTarget showing the steps involved in a traditional ransomware attack:



Another common technique is called a "double extortion ransomware attack," where the cybercriminal not only encrypts the data, but also exfiltrates the data to another location and threatens to share or disclose the data—often containing confidential or sensitive information—to others. Below is a diagram prepared by TechTarget showing the occurrence of events in a double extortion ransomware attack:



Who are Typical Targets of Ransomware?

No one is immune from attack when it comes to ransomware or security breaches resulting in loss of, or

unauthorized access to, data. However, over the past few years, certain industries falling within the sixteen critical infrastructure sectors often find themselves the victims of a ransomware attack. According to the United States Cybersecurity & infrastructure Security Agency ("CISA"), "[c]ritical infrastructure are those assets, systems, and networks that prove functions necessary for our way of life."[ii] The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. § 5195c(e)), namely "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Presidential Policy Directive/PPD-21 issued on February 12, 2013, by President Obama designated the following sectors as critical infrastructure sectors:

- Chemical;
- Commercial Facilities;
- Communications;
- Critical Manufacturing;
- Dams;
- Defense Industrial Base;
- Emergency Services;
- Energy;
- Financial Services;
- Food and Agriculture;
- Government Facilities;
- Healthcare and Public Health;
- Information Technology;
- Nuclear Reactors, Materials, and Waste;
- Transportation Systems; and
- Water and Wastewater Systems.[iii]

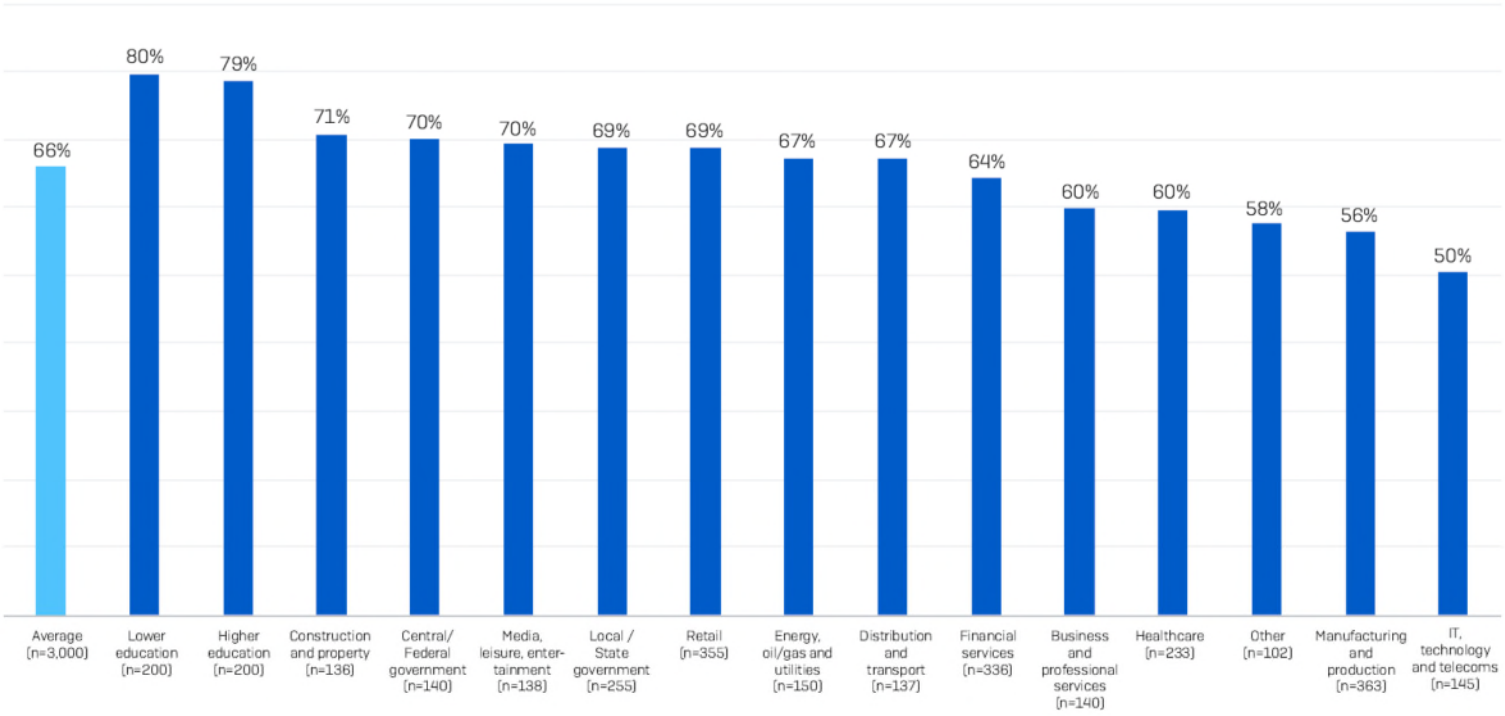
In the first quarter of 2023, Sophos, a British-based security software and hardware company, conducted a study of real-world ransomware events experienced by organizations with between 100 and 5,000 employees across fourteen counties in North and South America, Europe, the Middle East, Africa, and Asia Pacific.[iv] Participants were asked to respond based on their experiences with ransomware events over the previous year.[v]

Below is a graph displaying the percentage of organizations hit by ransomware between 2022 and 2023:

The State of Ransomware 2023

Rate of Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



In the last year, has your organization been hit by ransomware? Base numbers in chart

A Sophos Whitepaper. May 2023

When a business fitting within one of these critical infrastructure sectors is unexpectedly brought to a halt, the United States, and even the entire Globe, directly or indirectly feels the ripple effect. Because of the critical nature of operations, cybercriminals prey on the vulnerable nature of these organizations who are willing to pay exorbitant prices to their attackers to get back up and running in swift order. As the graph from Sophos portrays, you are more likely than not going to suffer from a ransomware event in the upcoming years.

Responding to the Ransomware Event Within Your Organization

Every second counts when your organization is brought to a standstill or unable to operate at full capacity. To quote Benjamin Franklin: "Time is money." When faced with a ransomware or denial of service event, businesses need a gameplan to follow to avoid wasting precious time and money (commonly referred to as an "incident response plan," as discussed in more detail in a later section). Below is a detailed overview of the responsive steps businesses take when experiencing a ransomware event. While the list is broken out into numerical steps, these steps frequently involve responsive actions that happen contemporaneously with one another and could vary in timing depending on each organization's priorities and whether cyber insurance coverage is available.

Step One: Initial Detection

The sophistication of cybercriminals varies as well as their techniques. Depending on the circumstances, cybercriminals may hurriedly copy a large pool of data, trying to grab as much information as possible, only to rapidly get out to avoid getting caught. While this "smash and grab" method does not require much skill and is often quickly detected, the victim still must investigate and respond to the security breach.

A cyber event involving ransomware often includes a clever and sophisticated criminal enterprise that is run like a business. Once ransomware infects a system, it can be difficult, if not impossible, to remove. These cybercriminals are intelligent and know how to infiltrate a system quickly and effectively, often going undetected for days, months, and sometimes years. In many cases, ransomware is detected only after it is announced by the cybercriminal, such as through a pop-up on the screen. However, signs of potential ransomware infection include:

- Alerts from anti-malware software;
- Lagging system performance;
- Blocked access to files;
- Anomalous network behavior and traffic;
- An increase in disk activity, as the ransomware script searches for and encrypts files on a system;
- Creations of new accounts, particularly privileged accounts;
- Installation of unauthorized software;
- Tampering of security systems and backups;
- Scanning of ports from inside a network; and
- Applications are not working properly because they depend on files that have been encrypted.

Step Two: Sound the Alarm!

Once an employee or representative of an organization detects a security breach or ransomware event, it is important to notify the applicable supervisor and information technology ("IT") person or team immediately. As discussed in more detail below, it is important for all employees or contractors working

for your organization to be trained on how to identify a cyberattack or other security event and know who to contact to report any suspected cyberattack or security event or suspicious activity.

If an organization has cyber insurance coverage, the organization must utilize the applicable breach hotline process as soon as practicable to report data breaches or other claims. The failure to timely report a potential data breach or claim could result in denial of coverage by an insurer.

U.S. businesses or individuals experiencing a ransomware event also should report it to the Internet Crime Complaint Center, applicable Federal Bureau of Investigation ("FBI") local field office, CISA incident reporting system, and/or United States Secret Service local field office as soon as possible. Be cautious when engaging with cybercriminals, as they are trained to manipulate you and prey on your weaknesses (e.g., inability to operate, lost revenue, reputational harm, etc.). The FBI and CISA, along with other government agencies, do not encourage victims of cybercriminals to pay the ransom because there is no guarantee that the cybercriminals will not use or disclose the data taken during the cyber event. Although, you may be familiar with the term "Honor Among Thieves," this is not always the case. Not everyone—especially cybercriminals—can be trusted.

Organizations experiencing a cyber event should engage legal counsel experienced in handling data breaches and familiar with reporting obligations. Often times, the deadline to report a data breach to various regulators is extremely short (see the subsection below discussing federal, state, and international reporting requirements). Organizations also have to be cognizant of their contractual notice obligations required in agreements with clients, customers, and other vendors. Such notice obligations are frequently found in business associate agreements with covered entities under the Health Insurance Portability and Accountability Act ("HIPAA"), software, platform, or other infrastructure service agreements, and financial agreements. Experienced legal counsel can help you navigate compliance with various reporting obligations simultaneously with recovery from an ongoing cyber event. If you have insurance coverage for a cyber event, it is likely that you will have experienced legal counsel included in your cyber response team.

Step Three: Isolate the Infected Device

Once a ransomware or other cyberattack is reported, an organization should immediately disconnect and isolate the affected systems from any wired or wireless connections, such as Internet, networks, mobile devices, flash drives, external hard drives, cloud storage accounts, network drives, or other equipment. The goal is to contain the ransomware or other computer virus and prevent it from spreading to other devices and throughout the network. Additionally, each device that was connected must be checked to see if it was likewise infected by the ransomware or virus. But be careful about immediately hitting the power-off button on the infected device, as this action may prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in the device's memory. CISA's checklist for responding to a ransomware event includes: "[o]nly in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection."[vi]

Step Four: Investigate the Ransomware

In many cases, a ransomware event or cyberattack will require a forensic investigation by security

professionals. Identifying the particular strain of ransomware or entry point for the cyberattack can help in remediation efforts. Experts in the cybersecurity field are familiar with various cybercriminals and ransomware organizations and may be able to navigate how to respond and quickly eradicate the ransomware or cyber threat. Being prepared to expediently investigate a ransomware event or cyberattack requires pre-planning and coordination with your cyber insurance provider, IT team, and/or cybersecurity services consultants. As discussed in more detail below, organizations should have an incident response plan and business continuity plan ready to deploy in the event of a cyberattack.

Step Five: Remove the Ransomware

Ransomware or other computer viruses must be removed before an organization can recover the infected system(s). During the initial hack, the cybercriminal's ransomware software infects a system and encrypts files and/or locks a system from access. The impacted organization cannot decrypt the files or unlock the system without a password or decryption key.

Options or remedies for removing ransomware include:

- Automatic Deletion. Occasionally, ransomware will delete itself after it has infected a system; however, this does not always occur.
- Anti-Malware or Anti-Ransomware Software. Most anti-malware or anti-ransomware software can quarantine and remove malicious software.
- Cybersecurity Professionals. Working with an experienced cybersecurity professional in your organization or through a third-party service provider will facilitate ransomware removal.
- Manual Removal. An experienced security professional may be able to manually remove ransomware by uninstalling the ransomware file on the infected device.

Even with removal of the ransomware software, your organization may still lack access to the encrypted files. Similar to preventative vaccines against flu and viral infections, not every decryption tool will combat every strain of ransomware. Sometimes decryption tools are not available to counteract the ransomware software utilized by the cybercriminal.

Additionally, it is important to perform comprehensive scans of a device or system to ensure no ransomware remnants remain that could infect the same device or system or spread to non-impacted devices or systems throughout the network. It may be necessary to quarantine or replace affected devices to ensure they are clean before restoring the applicable system or connection.

Step Six: Data Restoration

Alongside removal of the ransomware or other computer virus, it is equally important to begin restoring the compromised or lost data from backups in a secure environment. Contemporaneous data restoration in a secure environment offers your business the ability to pivot and regain access to encrypted data that is otherwise inaccessible due to the ransomware event. Organizations should back up all business-critical data as often as reasonably possible to reduce data loss and vulnerability when (not if) there is a ransomware or denial of service event. Security professionals recommend keeping at least one immutable data backup offsite and disconnected from the internet.

Step Seven: Recover and Rebuild the Infected System(s)

Once the threat of any remaining ransomware software or other computer virus is eliminated, your organization may commence recovering and rebuilding the impacted system(s). Restoration may include introducing the once-infected devices back into service and restoring data from backups. In some circumstances, the hardware will be damaged beyond repair and require replacement. Organizations often discover that system upgrades are also necessary during the rebuilding process.

After recovering the system(s), organizations should perform the following security measures as soon as possible to protect against another, sometimes larger ransomware or cyberattack:

- Update all passwords and security access codes (Note – individuals should avoid reusing passwords or using the same or similar passwords on multiple accounts, especially both work and personal accounts);
- Check to ensure firewalls and anti-malware software are up to date. It may be necessary to replace security software with stronger software or other security software depending on applicable lifecycles or known vulnerabilities;
- Debrief the ransomware event with your organization's executive team and employees to learn from the event and identify areas that require improvement, such as incident response plans, internal or external communications procedures, data security measures, employee training, etc.
- Follow the ransomware prevention measures described below or developed by your organization during the debriefing session.

While all ransomware or cyberattacks are costly and seem to happen at the worst times (often by design by the cybercriminal) it is important for your organization to gain knowledge and insight from an unfortunate event and come out stronger and more secure on the other side.

Impact on Your Business from the Ransomware Event

Ransomware events and other cyberattacks impact businesses and individuals in several ways, including necessary compliance with legal and contractual obligations, reputational harm, and internal disorder and diversion of already, limited resources. Again, it is important to have an incident response plan and experienced cybersecurity team in place before the event takes place. Being prepared and trained (as much as one can be) for a cyber event will reduce response time and additional stress in high-pressure situations.

Legal Implications and Duty to Report

In many cases, there are legal and contractual obligations that must be performed at a time where your organization is under intense pressure to recover from the ransomware event or cyberattack. Having a list in your organization's incident response plan or "cheat sheet" of potential notice deadlines and contact information for applicable regulators, clients, customers, or vendors is beneficial in times of need.

Federal Reporting Laws

Federal reporting obligations are often triggered based on governing laws or regulations applicable to certain industry sectors. Although not an exhaustive list, below are several examples of notice requirements applicable to the sixteen critical infrastructure sectors in the United States:

- United States Congress recently passed the Cyber Incident Reporting for Critical Infrastructure ("CIRCIA") Act, which requires a "critical infrastructure" company to report to CISA any "substantial cyber incident" within 72 hours after it "reasonably believes that the covered cyber incident has occurred."[vii] Additionally, ransom payments are to be reported within 24 hours.[viii] Federal contractors failing to monitor and report a cybersecurity incident, as required under CIRCA, may be subject to liability under the False Claims Act.[ix] Federal Regulation 52.239-1 requires contractors to "immediately" notify the government if they become aware of "new or unanticipated threats or hazards . . . or if existing safeguards have ceased to function".
- In July 2023, The United States Securities and Exchange Commission ("SEC") adopted final rules, effective September 5, 2023, that require a publicly traded company to determine the materiality of a cyber incident "without unreasonable delay" following discovery and, if the cyber incident is determined material, the company must file a Form 8-K, within four (4) business days of such determination.[x] The SEC final rule also requires companies to disclose annually information regarding cybersecurity risk management, strategy, and governance.[xi]
- In November 2023, the Federal Trade Commission ("FTC") published an amendment to its Standards for Safeguarding Customer Information ("Safeguards Rule"), 16 C.F.R. Part 314, requiring financial institutions to notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 consumers.[xii] This notice requirement applies to all financial institutions, including non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and lenders.[xiii] The FTC's amendment to the Safeguards Rule is effective on May 13, 2024.[xiv]
- Under 47 C.F.R. § 64.2011, the Federal Communications Commission ("FCC") directs covered telecommunications providers on how and when to disclose breaches of certain customer data to both law enforcement agencies and customers.
- The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires covered entities and their business associates to provide notification when there is a breach of unsecured protected health information. Notice must be given to:

  (i) affected individuals without unreasonable delay and in no case later than 60 days following discovery of the breach;

  (ii) the Secretary of Health and Human Services (either without unreasonable delay, and in no case later than 60 days, following discovery of the breach or on an annual basis depending on the size of the breach); and

  (iii) in circumstances involving more than 500 residents of a state or jurisdiction, to the media.

- The FTC also requires vendors of personal health records and their third-party service providers to provide similar breach notice provisions as covered entities under HIPAA, pursuant to Section 13407 of the Health Information Technology ("HITECH") Act.
- United States tax professionals experiencing a data breach must report the breach to the Internal Revenue Service ("IRS").[xv] Your local IRS Stakeholder Liaison coordinates IRS divisions and other agencies regarding a tax professional office data breach.[xvi] Tax preparers should also report a data breach to the FBI, United States Secret Service, and local law enforcement.[xvii]

State Reporting Laws

Reporting obligations are also dictated by the location or residence of impacted employees or consumers. All 50 states, Washington D.C., Puerto Rico, Guam, and the Virgin Islands have enacted data breach laws with various notice requirements in the event certain personal information or identifiers are accessed in a data breach. Applicable personal information or identifiers triggering notice requirements are dependent on the jurisdiction's data breach law, but often include:

- Social Security Numbers and other government identifiers,
- credit card and financial account numbers,
- health or medical information,
- insurance ID,
- tax ID,
- date of birth,
- online account credentials,
- digital signatures, and/or
- biometrics.

In cyber events involving exfiltration of data or unauthorized access to servers or files containing such personal information or identifiers, notice to the impacted individuals will almost always be necessary. Almost half of the states require notice to the applicable state Attorney General or designated official of certain data breaches. Additionally, in cyber events where more than 500 individuals are impacted, notice must be provided to credit bureaus, Equifax, Experian, and TransUnion.

International Reporting Laws

Many countries have their own reporting requirements in the event a data breach impacts one of its residents. Some examples include:

- Canada's federal privacy law for private-sector organizations, Personal Information Protection and Electronic Documents Act ("PIPEDA"), has breach notification requirements. Additionally, provincial privacy laws such as Alberta's Personal Information Protection Act ("PIPA") the Quebec Privacy Act require notice in the event of a qualifying data breach.
- Member countries of the European Union who have implemented the General Data Protection Regulation ("GDPR") require a "controller" of personal information to notify its supervisory

authority of a personal data breach without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the data breach is unlikely to result in any risk to a natural person's rights and freedoms.[xviii] In the event of a more serious data breach—likely to result in a high risk to a natural person's rights and freedoms, notice must also be sent to affected data subjects without undue delay.[xix]

- The Brazilian General Data Protection Law ("LGPD") requires a controller of data to report to the Brazilian National Data Protection Authority ("ANPD") and the data subject notice of a data breach if the breach is likely to result in risk or harm to data subjects.[xx] The LGPD itself does not set a specific deadline for notifying the ANDP in the event of security incidents, but requires reports within a reasonable timeframe. However, according to guidance published by the ANDP on February 22, 2021, most businesses must report the data breach within two (2) working days, counted from the date of receiving knowledge of the incident.[xxi]
- Under Japan's Amended Act on Protection of Personal Information (the "Amended APPI"), business operators shall report data breach incidents to the Japanese Personal Information Protection Commission ("PPC") and affected individuals if the data breach incidents could harm the rights and interests of individuals.[xxii] "The Amended APPI requires a business operator to submit a final report within 30 days from the recognition of a data breach (60 days is the deadline for data breaches likely to have been committed for an improper purpose, such as a cyberattack)."[xxiii] The PPC issued concrete guidelines requiring notice in the case of any of the following:

  (i) sensitive personal information is or likely to have been leaked;

  (ii) personal information that would cause financial damage by unauthorized use is or likely to have been leaked;

  (iii) data leakage by wrongful purpose is or likely to have been occurred; and

  (iv) data leakage incident that involves more than 1,000 data subjects is or likely to have been occurred.[xxiv]

Contractual Obligations to Provide Notice

In the digital age, organizations frequently rely on software providers and other third-party service providers to perform certain business functions necessary for the organization to operate or provide its own services or goods to end users or customers. These service arrangements involve the processing of personal information. With the rise of ransomware and cyberattacks, more and more organizations, service providers, vendors, and customers are including "breach notification clauses" in their agreements, which incorporate contractual obligations to provide notice of a security breach or suspected security incident within a certain period of time.

The following paragraph is an example of a breach notification clause customary in service agreements involving personal data of a customer:

- In the event Service Provider has actual knowledge of, or reason to believe that there has been, a security breach of the systems and/or media containing Customer Personal Data or systems used to provide the Services and/or any unauthorized Processing of, access to and/or loss of

> Customer Personal Data, or the media containing such Customer Personal Data, ("Security Breach"), Service Provider shall promptly, but within no more than 72 hours, notify Customer of such and shall use commercially reasonable efforts necessary including those as may be required by law, to contain such Security Breach and to prevent any further Security Breaches. Service Provider shall require its Third-Party Vendors and Subcontractors to comply with this clause.

It is important to keep copies of such contractual obligations or generate lists with contractual notice obligations in the event of a ransomware event or cyberattack. In many cases, access to files with electronic records or contracts will be unavailable during a cyber event involving a denial of service or encrypted data. The average time period for businesses suffering a ransomware event to get back up and running is 21 days. Depending on the applicable notice provisions, an organization may already be in default for failure to provide notice if it is unable to follow the applicable notice requirements due to the inability to access the contract. Furthermore, notice of a security incident might need to go to another department or other representative than your normal point of contact. If you do not have this information saved in a separate location, notice to the appropriate parties may be delayed because you cannot access the contract to follow the proper notice requirements.

Damage Control

High-profile or local cyberattacks in your jurisdiction often attract media attention, especially when they involve well-known organizations or a large number of affected customers. Although ransomware events and other cyberattacks are unfortunately, a regular occurrence these days, these types of events cause consumers to lose confidence in an organization or be hesitant to hire businesses or individuals who recently suffered a cyberattack. It is not uncommon for businesses to miss out on business opportunities or experience a decrease in stock prices or financial loss following a cyberattack. A cyberattack can also affect employee morale and cause finger-pointing within an organization.

Repairing reputational harm and resolving internal disorder within your business often follow a ransomware event. Prioritizing cybersecurity measures is critical for businesses to maintain customer trust, avoid negative publicity, and minimize the potential reputational damage that can result from a cyberattack. While not a bullet-proof solution, timely communications and transparency about a ransomware event or cyberattack often generate trust among clients, customers, and employees. Businesses must demonstrate that they care more about their own customers and their respective personal information than profitability. Communicating your organization's mitigation efforts and implementing strategies to tighten security and protect customer data from further attack also boosts confidence in your organization.

Learning From the Ransomware Event

On a positive note, successfully recovering from a ransomware event provides valuable, hands-on experience and training on handling a cyberattack and insight into your organization's weaknesses. Businesses should use this experience to learn and be better prepared for the next cyber event that lurks in the shadows.

Perform a Post-Breach Forensic Analysis

Like Company ABC in our case study, performing a post-breach forensic analysis will help your

organization identify security risks and take action to mitigate those risks. To start, organizations should use forensic techniques to discover and analyze how the cyberattack occurred and apply appropriate security measures to address and correct the vulnerability. Request your business's IT department or provider to gather output data from firewalls, intrusion detection systems, and anti-malware software for further analysis. Additionally, examine data from systems involved with the ransomware attack to determine what security measures worked and what did not.

Prepare an After-Action Report

After recovering from a ransomware event or cyberattack, your IT department, privacy officer, and/or designated security team should prepare an after-action report with a detailed breakout and review of all tasks performed and actions taken or not taken in response to the cyber event. After-action reports focus on "lessons learned" by the organization. The after-action report should include a section evaluating and answering the following questions:

- What actions were supposed to happen or be performed?
- What actions actually happened or were performed?
- Why were there discrepancies?
- What aspects of your organization's response worked?
- What activities or protocols did not work and why?
- What activities or protocols should be modified or added for next time?

Update Your Business's Internal Policies and Procedures

In many situations, an after-action report will evaluate the success of your organization's incident response plan. If your business does not have an incident response plan, it is time to create one. An incident response plan is a guide for employees with instructions about what to do and who to call during a cyberattack or other disaster. Below is TechTarget's recommended steps in a ransomware

incident response plan:

A business continuity plan compliments an incident response plan and addresses how a business will continue to operate and conduct business manually when electronic systems are compromised or unavailable. While business continuity plans must be tailored to your specific business needs, the following elements are typically found in every business continuity plan:

- background information about your organization and important functions and assets;
- identify potential risks that could cause interruption to business operations;
- how to use the plan, including guidelines as to when the plan will be initiated;
- important contact information for IT, forensic experts, management, and privacy or cybersecurity professionals;
- a revision management process that describes change management procedures and adaptations;
- the purpose and scope of the plan and each adaptation;
- policy information and training for general understanding;
- communication channels;

- identification of available technology and backups;
- checklists and flow diagrams;
- a glossary of terms used in the plan; and
- a schedule for reviewing, testing, and updating the plan.

After evaluation and discussion, the incident response plan and business continuity plan should be created or revised, as applicable, to include new scenarios and processes to address those actions or tasks that failed in the earlier cyber event. Your organization's staff should be given a copy of any new or revised plans or policies and trained on the new procedures.

Educate Your Employees

Businesses recovering from a cyber event should conduct risk assessments and security audits and perform disaster recovery tests on a regular basis to identify any continuing vulnerabilities or weaknesses within the network or data processing activities. Often times, your organization's employees are the weak link. Verizon's 2023 data breach investigation report stated "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering."[xxv]

TechTarget reports that the top three areas of employee training should include discussion about phishing emails, social engineering, and password use.

Phishing Attacks

Training your organization's employees on how to identify phishing emails and other fraudulent activity

is critical to reducing your organization's risk of attack. Below are some best practices to follow when trying to review a suspicious email or trying to determine if an email is legitimate:

- Check the Sender's Email Address. Scrutinize the sender's email address for any variations or misspelled domains. kdalke@hinklaw.com vs. kdalke@hinklaw.com These email addresses look identical. However, if you hover over each email address, you will see the second one uses a lowercase "i" in place of the lowercase "l" in hinklaw.
- External Emails. Many organizations turn on security features that identify emails originating from outside the organization. If your business uses this type of security setting, any email not originating from within your organization will be marked with a pre-set external warning in the email. If you receive an email purportedly from someone within your organization, but the email contains the external warning, this is a scam email.
- Examine Email Content. Pay close attention to the email's content. Be cautious of unsolicited requests for personal or financial information, urgent demands, or unsolicited attachments or links. Cybercriminals prey on a person's natural tendencies to want to help and do a good job for the employer. Phishing emails often create a sense of urgency, which heightens stress levels and makes the employee more likely to respond immediately without taking a pause to fully analyze the situation and spot a scam.
- Contact the Sender. If an email seems suspicious, verify its authenticity by contacting the purported or legitimate sender through alternative means. Calling the sender directly or communicating with the sender through a separate channel will help you determine if the sender actually sent the email. If the email includes an attachment or link, ask the sender to describe the attachment or link contained in the email.
- Do Not Forward. If you have a suspicious email, do not forward it to anyone. You should treat suspicious emails like a cold and not spread it.

By following these practices, your organization can minimize the risks associated with scam emails.

Social Engineering

Social engineering is an attempt to obtain physical or electronic access to information by manipulating people and preying on human tendencies. A very common type of attack involves a person, website, or email that pretends to be something it's not. A cybercriminal will often research a business to learn names, titles, responsibilities, and any personal information they can find. The cybercriminal then uses this research to call or send an email with a believable, but made-up story, designed to convince you to give certain information. During training, it is important to remind employees that they might find social engineering scams across from them at customer service counters, on the other end of telephone calls, or even sitting in nearby cubicles.

Password Hygiene

Training employees on strong password use and password hygiene is also critical to avoid compromised credentials. When a security breach occurs that reveals user credentials, such as login IDs and passwords, cybercriminals sell these credentials on the dark web multiple times. Cybercriminals then

take these credentials and use them to try and hack into various other accounts or systems across the Internet. Employees who reuse passwords across multiple applications and accounts risk exposing corporate credentials. For example, if an employee uses the same login ID (such as an email address) and password to log on at work and for an online clothing merchant where an employee shops, this makes the employer vulnerable if the online clothing merchant suffers a security breach. Educating employees about safe password usage and practices will build awareness of the cyber risks associated with weak and/or reused passwords.

Training Techniques

Practice makes perfect! Cybersecurity training and awareness should be an ongoing process that your organization is committed to pursuing. Training must start with the onboarding process and continue throughout an employee's tenure at the organization. Make training interesting and relevant for your employees. While cybersecurity training may seem daunting or unnecessary, it is crucial to maintaining a secure work environment and often required by insurers and vendors or clients to conduct business.

Tabletop exercises are a great training tool. Tabletop exercises are designed to take participants through a simulated cyber incident scenario and provide hands-on training for participants that highlight flaws in incident response planning. Tabletop exercises often assist employees in understanding and identifying social engineering tactics used by cybercriminals to manipulate employee action. CISA is a great resource when it comes to table top exercises for your organization and provides several scenarios to choose from at https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios.

People learn in different ways, and it is important to include a variety of training options and techniques for building the best cybersecurity training program. In addition to tabletop exercises, below is a list of training options and techniques that make it easy for employees to learn and retain instruction on good cybersecurity practices:

- Live training, either in person or via video conferencing.
- On-demand video training.
- Interactive training and gamified training modules, available from third-party service providers.
- Regular newsletters that share cybersecurity and cybercrime news—e.g., recent data breaches, new phishing threats and enterprise security policy updates.
- Dedicated channels on collaboration platforms, such as Microsoft Teams or Slack, where users can find security content and news.
- Short discussions in team meetings about cyber hygiene and security awareness.
- Educational lunch-and-learn sessions.
- Informational posters in high-traffic areas of the office, such as kitchens and break rooms.
- Easy-to-read and accessible documentation that recaps cyber hygiene best practices and organizational cybersecurity policies.

Keep track of training performance and completion for each employee or department. Regulators, insurers, lenders, vendors, and even clients may request documentation related to employee training and completion. Utilizing employee training records may help mitigate the impact on your business from a cyberattack or demonstrate that your organization poses less security risks than its competitors.

Take Proactive Steps to Minimize a Cyberattack or Prevent it From Occurring in the First Place

Just like many sports, the best defense to a cyberattack is a strong and ready offense. It is crucial for your organization to be proactive and take preventative measures to minimize the impact of a ransomware event or other cyberattack. The following guidance includes best practices relevant to most industries and all critical infrastructure sectors:

- Use separate personal and business computers, mobile devices, and email accounts. This is especially important if other people, such as children, use personal devices. Do not conduct business or any sensitive activities (like online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to personal email addresses.
- Use strong passwords. Strong passwords consist of a random sequence of letters (upper- and lower-case), numbers, and special characters. The National Institute of Standards and Technology ("NIST") recommends passwords be at least 8 characters long when used with other authenticators, although NIST's recommendations are continuously evolving. Phrases or sentences with numbers and characters are harder to crack than single word passwords. Passwords should be changed at least every three (3) months. Passwords to devices and applications that deal with business information should not be re-used or used for personal accounts.
- Use multi-factor or dual-factor authentication tools. For systems or applications that have important information, use multiple forms of identification (called "multi-factor" or "dual factor" authentication). Multi-factor authentication combines two or more independent credentials: (1) what the user knows, such as a password; and (2) (a) what the user has, such as a security token or code and/or (b) what the user is, by using biometric verification methods, such as a thumbprint or face recognition. Multi-factor authentication provides a layered defense, which makes it more difficult for a cybercriminal to gain access to a system or device because the cybercriminal has to have all credentials and necessary components to gain access.
- Secure and encrypt data at rest and in transit. Any paper records containing personally identifiable information ("PII") and/or confidential information should be secured appropriately when not in use. Organizations should implement a clean desk policy when possible, by instructing employees not to keep files containing such PII or confidential information open on their desks when they are not at their desks. Any computer file stored on a business network containing PII or confidential information should be password-protected and/or encrypted. Keep computers and devices locked from access when not in use. Use secure email accounts and

encrypt PII and confidential information when transferring it to another co-worker or external third-party via email.

- Do not connect personal or untrusted storage devices or hardware into computers, mobile devices, or networks. Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown/untrusted hardware into your organization's system or network, and do not insert any unknown CD, DVD, or USB drive. Disable the "AutoRun" feature for the USB ports and optical drives like CD and DVD drives on business computers to help prevent malicious programs from installing on the systems. Work with your organization's IT department to scan unknown or untrusted hardware or drives before connecting it to your system.
- Be careful downloading software. Do not download software from an unknown web page. Be very careful with freeware or shareware.
- Watch out when providing personal or business information. Be cognizant of social engineering tactics. Never respond to unsolicited phone calls that ask for sensitive personal or business information. Do you not give out codes or links used to verify your identity to third parties. Employees should notify management and IT whenever there is an attempt or request for sensitive business information. Never give out usernames or passwords. No company should ask for this information for any reason. Also, beware of people asking what kind of operating system, brand of firewall, internet browser, or what applications are installed on your organization's network and systems. This is information that can make it easier for a cybercriminal to hack into the system.
- Watch out for harmful pop-ups and be careful where you click. When connected to and using the Internet, do not respond to popup windows requesting users to click "OK." Use a popup blocker and only allow popups on trusted websites.
- Conduct online business more securely. Online business, commerce, and banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of the web browser window. Erase the web browser cache, temporary internet files, cookies, and history regularly. Typically, this is done in the web browser's "privacy" or "security" menu. Review the web browser's help manual for guidance. Ensure to erase this data after using any public computer and after any online commerce or banking session. These practices prevent important information from being stolen if the system is compromised.

[i] National Cyber Investigative Joint Task Force, *Joint-Seal Ransomware Fact Sheet*, available at https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf, accessed on Dec. 30, 2023.
[ii] United States Cybersecurity & infrastructure Security Agency, *Critical Infrastructure Security and Resilience*, available at https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience, accessed on Dec. 30, 2023.
[iii] Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed on Jan. 3, 2024.
[iv] SOPHOS, *The State of Ransomware 2023*, available for download at https://www.sophos.com/en-us/content/state-of-ransomware.
[v] *Id.*
[vi] United States Cybersecurity & infrastructure Security Agency, *Ransomware Response Checklist*, https://www.cisa.gov/ransomware-response-checklist, accessed on Dec. 30, 2023.
[vii] Cyber Incident Reporting for Critical Infrastructure Act of the 2022 Consolidated Appropriations Act, Pub. L. No. 117-103, div. Y (Mar. 15, 2022), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.
[viii] *Id.*
[ix] *See* Dep't of Justice, Office of Pub. Affairs, *Justice News: Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, (Oct. 6, 2021), available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative, accessed on January 3, 2024.
[x] *See* Security Exchange Commission, *Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure* (Modified Nov. 14, 2023), available at https://www.sec.gov/corpfin/secg-cybersecurity; *see also* Security Exchange Commission Release Nos. 33-11216; 34-97989, at 12 (July 26, 2023).
[xi] *Id.*
[xii] Federal Trade Commission, *Final Rule to Amend the Safeguards Rule*, 88 FR 77499, at 77505 (Nov. 13, 2023), available at https://www.federalregister.gov/d/2023-24412/p-96.
[xiii] *Id.*
[xiv] *Id.*
[xv] Internal Revenue Service, *Tax Tip 2023-106* (Aug. 30, 2023), available at https://www.irs.gov/newsroom/tax-professionals-must-act-fast-after-discovering-a-data-breach#:~:text=How%20to%20report%20a%20data,on%20the%20tax%20professional's%20behalf, accessed on Jan. 1, 2024.
[xvi] *Id.*
[xvii] *Id.*
[xviii] *See* GDPR, Art. 34.
[xix] *Id.*
[xx] LGPD, Art. 48.
[xxi] *See* International Bar Association, *The Brazilian National Data Protection Authority's Established*

Guidelines on Best Practice Regarding Data Breaches (Aug. 2, 2021), available at https://www.ibanet.org/aug-21-brazilian-data-protection-authority, accessed on Dec. 31, 2023.

[xxii] International Association of Privacy Professionals, *Practical notes for Japan's important updates of the APPI guidelines and Q&As* (Jan. 10, 2022), available at https://iapp.org/news/a/practical-notes-for-japans-important-updates-of-the-appi-guidelines-and-qas/, accessed on Dec. 31, 2023.

[xxiii] *Id.*

[xxiv] *Id.*

[xxv] Verizon, *2023 Data Breach Investigation Report*, available for download at https://www.verizon.com/business/resources/reports/dbir/?cmp=knc:ggl:ac:ent:ea:na:8888855284&utm_term=2023%20verizon%20dbir&utm_medium=cpc&utm_source=google&utm_campaign=GGL_BND_Security_Exact&utm_content=DBIR2023&ds_cid=71700000082347933&ds_cid=&gad_source=1&gclid=CjwKCAiAqNSsBhAvEiwAn_tmxThou2vQ9bsJi-8a0nL_a2-weq_ekeOYDKoqcL9KNfKeRAyA1vSY1hoCg3cQAvD_BwE&gclsrc=aw.ds.