2024 Business Litigation Practice Group Seminar

September 11-13, 2024

We've Been Hacked!

Choose Your Own Adventure Navigating a Data Breach

Cody J. Cooper
PHILLIPS MURRAH P.C.
Oklahoma City, Oklahoma
cjcooper@phillipsmurrah.com

Krystle Dalke, J.D., CIPM, CIPP/US
HINKLE LAW FIRM LLC
Wichita, Kansas
kdalke@hinklaw.com

Introduction

"We've been breached!" Words that no submarine operator or business executive ever wants to hear. Cybersecurity incidents and breaches are becoming commonplace to the point where if you said you haven't already experienced a breach or cybersecurity incident, you either don't realize that its already occurred, or you are lying. The grim reality is that breaches are becoming more and more frequent from increasingly more creative and complex avenues. It is estimated that over 1 billion records have already been stolen as part of cyber incidents so far this year. Now, add in all that Artificial Intelligence can do into the mix and you have a recipe for disaster for businesses and their third-party vendors. Companies' scope of data continues to grow at what feels like an unsustainable pace. While this can provide significant business advantages and developments, it also significantly increases the risk of a debilitating cybersecurity breach. On top of that, the cost for responding to data breaches continues to increase, with the average cost of a data breach estimated at $4.88 million dollars.[1]

Below are the general steps that a company goes through when it has experienced a reportable data breach. Although these are listed in numerical order, oftentimes in practice these do not flow nicely in order but are addressed contemporaneously in frenzied efforts. Additionally, there may be unique circumstances that call for different actions that may not be covered in this article. However, the steps identified below are based on experience with breaches ranging from all ends of the gambit and the practical experience of the attorneys that handled these issues.

Step 1: Identify a Potential Breach Has Occurred.

Fortunately, the majority of cybersecurity incidents are avoidable. There are numerous different types of attacks and companies should be mindful of instituting policies and practices to educate their employees in order to best avoid data breaches and/or detect cybersecurity incidents. The most common types of cyber-attacks include:

- Dos and DDoS (Denial of Service)
- MITM (man-in-the-middle) attacks
- Phishing/Smishing/Whale-Phishing/Spear-Phishing
- Ransomware
- Password attacks
- Insider threats
- DNS spoofing[2]

Unfortunately, the odds heavily favor that most companies and individuals have or will experience some sort of cybersecurity incident. When that does occur, it is critical to recognize it as soon as possible and act quickly to contain the effects. General best practices are that any time someone suspects there is or could be a breach to immediately report it to the appropriate company personnel. Often, this is the IT group either using a specific point of contact or a specific group of individuals.

Recognizing that a breach has occurred or is occurring is oftentimes the most obvious step of any

[1] Cost of a Data Breach Report 2024, available at https://www.ibm.com/reports/data-breach.
[2] Types of Cyber Attacks, available at https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks.

cybersecurity incident, but it is frequently not recognized soon enough. Most times, a company realizes it is experiencing a cybersecurity incident because of facially obvious issues (i.e. systems are locked out and/or unavailable or a ransom note is shown in a client's system). When an employee does suspect a breach has occurred, they should immediately disconnect the device from the internet service and power it off. They should then immediately notify the appropriate individual in the company's IT group in order for that individual to initiate the process of investigating the potential issue. Then, in the event of an actual breach, IT should escalate the issue up the chain of authority to the appropriate individuals to start the breach notification investigation and analysis.

In addition to ensuring that a company's information technology infrastructure is as harden as possible against attacks and constantly up to date on security patches, it is equally critical that companies provide regular training with employees on how to quickly recognize and respond to suspicions of a cybersecurity incident. This training should include how to spot suspicious emails and links, what can and cannot be downloaded to company devices, and who to notify in the event of a cybersecurity incident. While no system is breach-proof, up-to-date IT security practices, along with trained and educated employees, will give a company the best shot to avoid a data breach in the first place.

Step 2: Alert Relevant Stakeholders

Once an employee or representative of an organization detects a cybersecurity incident, it is important to alert relevant stakeholders immediately. Relevant stakeholders often include both internal and external parties, such as executives, managers, internal IT teams and outside security consultants, general counsel, forensic experts, HR, and public relations. If an organization has cyber insurance coverage, the organization must utilize the applicable breach hotline process as soon as practicable to report suspected 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.

Organizations experiencing a cyber event also should engage outside legal counsel experienced in handling data breaches and familiar with notice and reporting obligations in relevant jurisdictions. 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 must also 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.

U.S. businesses or individuals experiencing a ransomware event or cybercrime may also 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. Reporting cybercrimes to law enforcement allows them to investigate, track cyber threats, and even freeze or recover stolen funds.

It is important for all employees or contractors working within your organization to be trained on how to

identify a cyberattack or security incident and know who to contact to report any suspected cyberattack or suspicious activity without delay. Organizations should include a call tree in their incident response plans with key stakeholder names, titles, and/or positions, office and cell phone numbers, and other applicable contact information. This information must be current and maintained on an ongoing basis to be effective during an actual security incident.

Step 3: Commence Triaging IT and Business Functions

Isolate the Infected Device or System

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 malware and prevent it from spreading to other devices, systems, and throughout the network. Additionally, each device that was connected to the infected system must be checked to see if it was likewise infected by the malware. 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."[i]

Remove the Malware

Ransomware or other computer malware 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.

Data Restoration

Alongside removal of the malware, it is equally important to begin restoring the compromised or lost data from backups in a secure environment. Contemporaneous data restoration offers your business the ability to pivot and regain access to encrypted data that is otherwise inaccessible due to the cyber 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 cyberattack. Security professionals recommend keeping at least one immutable data backup offsite and disconnected from the internet.

Step 4: Identify and Review Insurance Policies And Notify Carrier(s)

While many of these initial steps will occur simultaneously, it is vital to ensure that someone on your response team is vetting your insurance coverage, notifying your carrier of the breach, and then working directly with the carrier to ensure that any applicable and necessary coverage is obtained. In order to do this, it is vital that companies understand what policies are in place that could potentially provide insurance coverage under the various scenarios and also what that policies will cover and what amounts. Equally vital is understanding what is excluded under those policies. It is then important to incorporate your counsel to ensure that everyone understands the policies and their language as you all collectively work through the breach process and coordinate those efforts with your carrier to effectively and efficiently respond to the breach, repair the issue, and strategically move to place yourself in the best position following the breach.

Understand the Applicable Policies and Familiarize Yourself with Coverage

Typically, cybersecurity polices may cover things like:

- Customer notifications
- Recovering personal identities
- Data breach investigations (i.e. forensic examinations, attorneys' fees, etc.)
- Data recovery
- System damage repair
- Ransom demands
- Attack remediation
- Liability for losses incurred by business partners with access to business data

Like all insurance policies, the devil is in the details. Insurance coverage for cybersecurity incidents is becoming more expensive and more difficult to procure, with carriers frequently requiring a showing of appropriate security measures and asking thorough questionaries about a company's IT security practices and procedures. Even then, policies are limited in coverage and typically have numerous sublimits for different exposures. Examples of common sublimits include response expenses, public relations, legal review, regulatory fines, ransom payments, loss of business and others.

It is very likely that your carrier has panel counsel and vendors with whom it regularly does business on cyber matters, and the carrier may require you to use their preferred vendors. Even though your carrier may have preferred partners to assist, you can always request to engage counsel and vendors with whom you are familiar. In this instance, your carrier will vet the firm or vendor and also likely require that they agree to the panel rates that their pre-approved partners use on similar work. This is one way to be able to work with your insurance carrier and firms and companies with whom you are familiar and comfortable.

Pay Close Attention to the Exclusions in the Policy

Insurance policies do not cover every possible loss, and even when they do apply, there are frequent exclusions for certain events and/or costs. Companies should be intimately familiar with their policies when presenting claims in order to ensure that they communicate effectively with the carrier to provide necessary information to confirm coverage exists and ensure payment of covered items.

Common exclusions under cybersecurity policies include:

- Poor security processes: If an attack occurred as a result of an organization having poor configuration management or ineffective security processes in place
- Prior breaches: Breaches or events that occurred before an organization purchased a policy
- Reckless conduct: Any cyberattack caused by reckless conduct by an organization's employees
- Insider attacks: The loss or theft of data due to an insider attack, which means an employee was responsible for the incident
- Preexisting vulnerabilities: If an organization suffers a data breach as a result of failing to address or correct a previously known vulnerability
- Technology system improvements: Any costs related to improving technology systems, such as hardening applications and networks

Again, policy terms and any applicable sublimits will dictate both what cost items are covered and the dollar limitation on that coverage. Companies should be mindful of these when negotiating coverage and also keep in mind the potential exposure that could exist if their systems are compromised. The most sensitive information a company keeps, the higher the potential exposure the company would face in the event of a breach. Companies should purchase policies that align with their specific risk profile to ensure that they have the most efficient coverage possible.

Step 5: Engage Outside Vendors

On a positive note, successfully recovering from a cyberattack 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. Regulators, clients, and consumers will appreciate knowing your organization took action to improve its security processes to protect information from further exposure in the future.

Forensic Examination

There are many large companies that specialize in cybersecurity services specifically including forensic examination of computer systems. These companies have the capability of reviewing your systems and

individual devices to search of evidence of a breach and also how it occurred. These vendors are critical to the process of remediation and understanding the nature of the breach. Unless there are explicit signs of what information was accessed and/or stolen (i.e. ransomware showing you a copy of the information they possess), a forensic examination can be the only way to determine the nature and scope of the breach.

Breach Counsel

Engaging counsel to assist in the investigation is critical. Seasoned and experienced counsel can assist in triaging systems and understanding how to prioritize immediate needs beyond data restoration and company operations. In these situations, companies and their employees necessarily and appropriately prioritize business continuity and restoring access to critical systems. While this is imperative for the ongoing operations of the company and its customers and business partners, there are critical legal decisions that have to occur in real-time in order to ensure both compliance in the present and strategic positioning in the event of future litigation.

IT Vendor

Depending on the depth of a company's IT group and the complexity of the breach, there may be times when a company needs to engage an outside vendor to assist in system recovery and remediation. There are outisde IT vendors that can assist with setting up new devices, fixing firewall settings, reconnecting servers, updating security settings, ensuring up-to-date security patches and any number of additional measures to assist companies and individuals to get their systems and devices back up and running as quickly as possible.

Notification Vendor

There are companies that specialize in cybersecurity notification services. These companies help sort the individuals to be notified along with their contact information then finalize the actual notification to be provided to each (obviously after sign off from the company and breach counsel to ensure notification compliance) and then they physically handle the notifications to affected individuals by mailing all of the notifications.

Public Relations Firm

Depending on the scope and severity of a cyber security incident, companies may want to hire a public relations firm to handle public communications and public statements. Obviously, any public statements should also involve breach counsel to ensure that the statements do not cause legal issues in the present or in the future should litigation occur.

Step 6: Identify the Nature of The Breach

During the breach investigation, the forensic examiner will examine the company's systems to determine what portions of the system were affected and ultimately how the cybersecurity incident occurred. It is important to attempt to identify the nature of the breach so that the company can understand why its systems were compromised and also so that it can report to the appropriate law enforcement and administrative agencies.

Understanding how the cybersecurity incident occurred is helpful to a company in order to narrow what portions of its network have been affected but also in order to understand how to harden the company's system to prevent that same issue from occurring again.

Being able to report to law enforcement how the breach occurred will also allow law enforcement to investigate the issue and look for patterns with other reported breaches to determine if there is a connected group of breaches by a group or using common means. This will assist law enforcement in their investigation and hopefully assist in preventing future breaches.

Step 7: Remediation Efforts from the Cyber Event

Cyber events and other security incidents 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. Organizations must remediate the cyber event by promptly addressing the security incident and mitigating the potential damage resulting from the security incident. The goal is to restore normal operations as soon as possible while also fixing weaknesses and vulnerabilities and taking preventative measures to prevent future breaches or cyber events. Your organization will also need to identify the root cause of security risks and determine its risk tolerance for potential incidents. Again, it is important to have an incident response plan and experienced cybersecurity team—e.g., internal and external IT professionals, forensic experts, legal counsel, and cyber insurance carrier—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.

Step 8: Identify Scope Of The Breach

During the forensic analysis, it is vital that a company's vendor determines what area of the network, systems, servers, and databases are—or potentially are—affected. This is critical because without understanding what areas of a company's systems are implicated, it is impossible to narrow down what data could have been potentially exposed which will necessarily result in a company have to guess as to the scope of notifications. By narrowing the affected area as precisely as possible, a company can then begin the process of determining whether any personally identifiable information is implicated, the jurisdictions implicated, and the number of individuals possibly affected. This will dictate the necessary steps a company has to take to determine whether breach notifications are even required. This process should be handled directly in coordinated efforts by your forensic examiner, internal IT individuals, and breach counsel to determine the scope of affected areas and be comfortable with that determination so that it if it is later questioned by administrative bodies or in litigation then conclusion can be supported and defended.

Step 9: Notify Requisite Law Enforcement and Administrative Bodies

This step can and should be moved up in most instances, but again, it is a case-by-case decision. Best practice is to notify law enforcement as soon as possible. But which law enforcement agencies do you notify? Even more, depending on a company's area of business, they may have obligations beyond simply notifying the affected individuals.

Law Enforcement

Companies should notify local law enforcement as well as the FBI's Internet Crime Complain Center, which can be found at https://www.ic3.gov/. You can also contact the United States Secret Service because it shares responsibility for investigating cybercrimes. If the incident involves mail theft, then the company should contact the United States Postal Inspection Service. Companies should be mindful of what they report to law enforcement to ensure complete accuracy but also to ensure that what they report to law enforcement is consistent with any public statements and the notifications that are ultimately provided individuals. Oftentimes, notifications to law enforcement are early on before companies have the full scope of the picture and all factual information. These communications are not generally privileged or protected from discovery so it is incumbent on companies that they make this clear in any written notification to law enforcement so that they do not make any misstatements that are later used against them in a lawsuit.

Governmental Notifications

Depending on the states impacted and the size of the breach, as well as a company's area of business, companies may have additional obligations to notify governmental and administrative agencies of the cybersecurity incident. Some states require companies notify their state's Attorney General and also require the affected company to notify "all consumer reporting agencies."[3] Some breaches also require notification to the Federal Trade Commission (and in some cases the media). If the information is protected information under HIPAA, then the company may also have to contact and the Secretary of the U.S. Department of Health and Human Services (HHS).[4]

Step 10: Analyze Scope of Individuals and Entities Affected

Generally, data breach notification requirements are triggered when "personally identifiable information" is acquired or authorized by someone who is not authorized to access the information. Once the breach notifications are tried and in order to start the notification process, a company experiencing a breach has to determine who must be notified. This steps necessarily includes identifying the identities of the individuals affected, the information that was affected, the number of individuals, and the residence of the individuals affected.

Number and Nature of Individuals and Entities Impacted

Data breach statutes generally speak to notifying individuals, not necessarily companies. Yet, contractual provisions may trigger breach notifications, and it is generally good business sense to notify companies their information has been breached. It is also beneficial to try to narrow the group of individuals to be notified to be as narrow as possible (based on the information discovered during the breach investigation). In order to do all of this, the company must determine the individuals and entities that are affected, as well as the categories of information that have been affected. For example, if only names and addresses are affected, that very likely does not necessitate breach notification because this information is not considered to be "personally identifiable information." The easiest way to think about what

[3] Data Breach Notification Laws by State, available at https://www.itgovernanceusa.com/data-breach-notification-laws.
[4] Data Breach Response: A Guide for Business, available at https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

information likely triggers notice obligations is to think about what information is generally publicly available through a telephone book (if those are even a thing anymore) or through a generic Google search. Oftentimes, these categories of information will not require a notification even if they are accessed by someone who does not have authority.

Residency of the Impacted Individuals and Entities Impacted

Aside from industry-specific requirements, which data breach notification laws will apply will largely be driven by the residency of the individuals affected. At this point, every state has its own breach notification statute and many of them overlap, but they are still patchwork and some have stricter standards. Even more, some industries have regulations that may be implicated by their regulatory bodies which could provide a different standard than the applicable state laws. Examples of these include Gramm Leach Bliley, the National Credit Union Administration guidance, HIPAA, FTC guidance and others. Countries also can have significantly different data breach notification requirements. The prime example here is the General Data Protection Regulation (GDPR) that applies to European Union residents which has detailed, stringent, and far-reaching obligation. Failure to comply with each of these different statutory regimes can result in significant liability to an unknowing company and it is important to ensure that your breach counsel is familiar with the various statutes to ensure compliance with the same.

Step 11: Notification Process

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 remediate the 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 passed the Cyber Incident Reporting for Critical Infrastructure ("CIRCIA") Act in 2022, 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."[ii] Additionally, ransom payments are to be reported within 24 hours.[iii] Federal contractors failing to monitor and report a cybersecurity incident, as required under CIRCIA, may be subject to liability under the False Claims Act.[iv] 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". CIRCIA is currently in the process of receiving public comments for final rulemaking.
- 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.[v] The SEC final rule also requires companies to disclose annually information regarding cybersecurity risk management, strategy, and governance.[vi]

- 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.[vii] This notice requirement applies to all financial institutions, including non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and lenders.[viii] The FTC's amendment to the Safeguards Rule is effective on May 13, 2024.[ix]
- 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").[x] Your local IRS Stakeholder Liaison coordinates IRS divisions and other agencies regarding a tax professional office data breach.[xi] Tax preparers should also report a data breach to the FBI, United States Secret Service, and local law enforcement.[xii]

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.[xiii] 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.[xiv]
- 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.[xv] 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.[xvi]
- 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.[xvii] "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)."[xviii] 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.[xix]

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.

Step 12: Staying Updated On the Notification Process

During the notification process, it is important that the breach counsel and the company pay attention to and track the progress of the notifications of the affected individuals. Even though you will likely have a vendor handling this process, it is incumbent to understand the locations and the number of individuals who have been notified in order to ensure compliance with the various data breaches laws referenced above. It is also possible that the governmental agencies may request updates as it relates to the progress of notifications.

Step 13: Defending Potential Lawsuit

There is always a chance that a lawsuit will develop after any breach. Suits arising from a beach typically are brought as a collective action or a class action.

Common Claims

The most common claims are for negligence, breach of contract, negligence *per se*, and fraud. Negligence claims are typically based on the argument that the company owed a duty of care to protect plaintiffs' personally identifiable information and breached that duty and damaged plaintiffs as a result. Breach of contract claims are occasionally based on agreements that may mention protecting plaintiffs' data or terms of use that reference use of a company's system and the security of the same. Plaintiffs often try to allege that a breach notification standard or general regulation equate to standards that are mandatory and can provide the basis for negligence *per se* claim. Finally, the fraud claims are often premised on the argument that the company represented their software/product/system was safe to use but it was clearly not since plaintiffs' data was breached therefore, the company committed fraud by misrepresenting their software/product/system.

Discovery

Discovery in these cases will inevitably focus on several categories of information that will obviously vary based on the exact nature of the claims and how the breach occurred, but the two primary areas of discovery will be: (1) IT security practices and (2) the breach investigation and response. Both broad categories interplay with privilege protection and attorneys should be mindful of the potential applicable privileges while handling a cybersecurity incident.

The work-product doctrine is intended to protect things from disclosure that were prepared for or in anticipation of litigation. Similarly, the attorney-client privilege protects communications between a client and attorney where the communications are for the purpose of obtaining or providing legal advice. Privilege can extend beyond only attorneys and their clients and also include agents that assist in facilitating the attorney-client communications or representation. These privileges are generally disfavored and construed narrowly, and they play a role in the discoverability of cybersecurity investigations.

Obviously, IT security practices generally won't have any applicable privilege that attaches to them but that may not be the case related to the forensic examination and it is critical to consider this during the investigation process to best position yourself in litigation.

Standing, Causation and Damages

"Plaintiffs typically seek damages for unauthorized charges, damage to credit, cost of credit monitoring, cost of replacement credit cards, time and expenses incurred to investigate, and emotional distress. Whether breach victims have suffered actual injury and cognizable damages to have standing to sue is the critical issue in many cases."[5]

At this point, nearly everyone has already been involved in a data breach and experienced their information leaking or becoming publicly available which makes it difficult for a plaintiff to tie their alleged damages directly to any one breach. Obviously, this makes surviving a motion for summary judgment or presenting at trial extremely difficult in order to prove your case as a plaintiff and provides ample opportunity for a defendant to point the finger at the many breaches that occurred before the one they experienced. This issue muddies data breaches cases and amplifies the need to extensive discovery and expert testimony which only increases the costs involved in these cases – on both sides of the v.

Step 14: Learn from the Cyber Event

On a positive note, successfully recovering from a cyberattack 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. Regulators, clients, and consumers will appreciate knowing your organization took action to improve its

[5] Data Breaches, available at https://www.sgrlaw.com/ttl-articles/data-breaches/#:~:text=Plaintiffs%20typically%20seek%20damages%20for,to%20investigate%2C%20and%20emotional%20distress.

security processes to protect information from further exposure in the future.

Perform a Post-Breach Forensic Analysis

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 cyber event, 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

Use the after-action report to update and improve your organization's internal policies and procedures. In many situations, an after-action report will evaluate the success of your organization's existing incident response plan and business continuity plan. After evaluation and discussion, the incident response plan and business continuity plan should be revised (or, at the very least, created) 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.

[i] United States Cybersecurity & infrastructure Security Agency, *Ransomware Response Checklist*, https://www.cisa.gov/ransomware-response-checklist, accessed on Dec. 30, 2023.
[ii] 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.
[iii] *Id.*
[iv] *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.
[v] *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).
[vi] *Id.*
[vii] 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.
[viii] *Id.*
[ix] *Id.*
[x] 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.
[xi] *Id.*
[xii] *Id.*
[xiii] *See* GDPR, Art. 34.
[xiv] *Id.*
[xv] LGPD, Art. 48.
[xvi] *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.
[xvii] 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.
[xviii] *Id.*
[xix] *Id.*