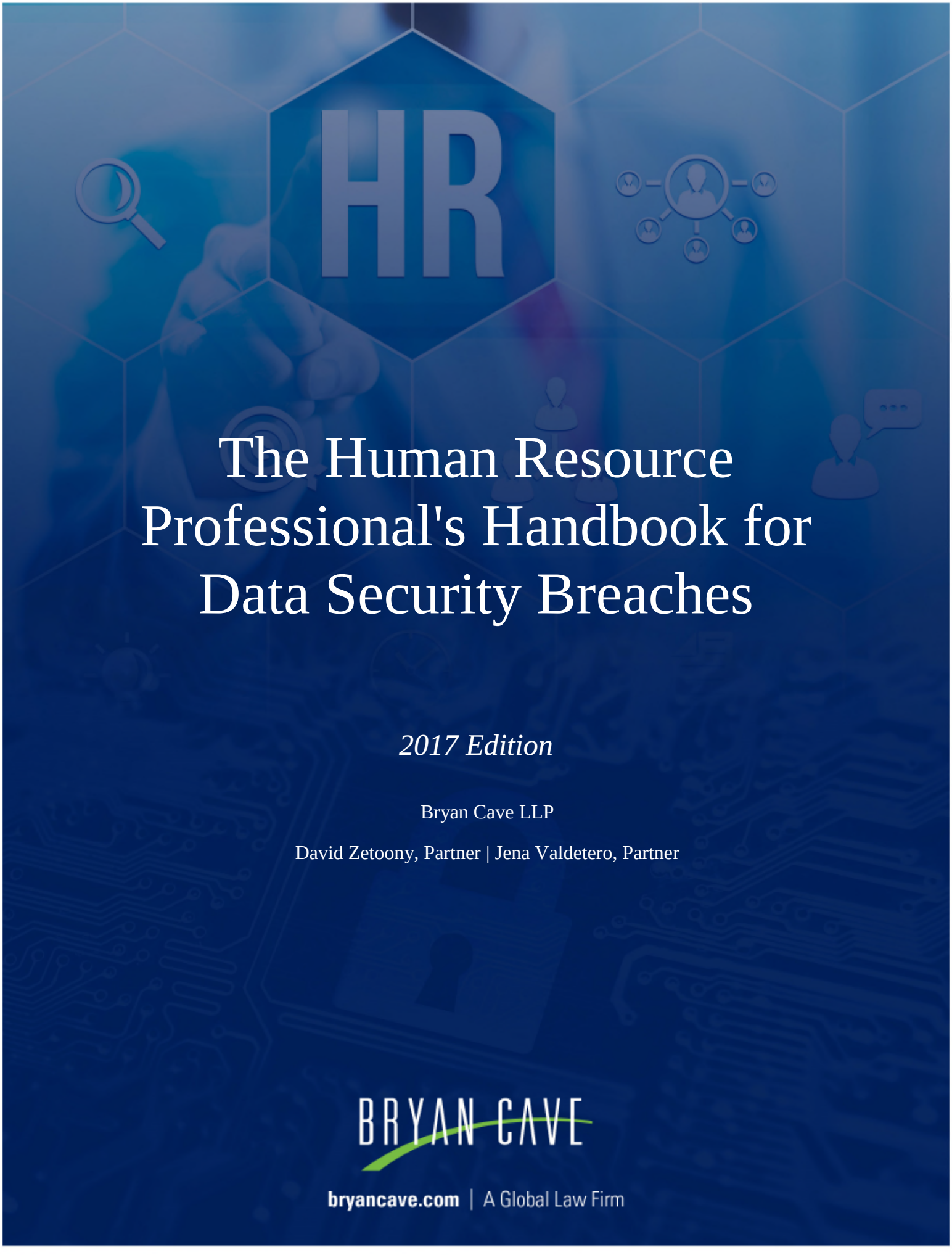


The Human Resource Professional's Handbook for Data Security Breaches

2017 Edition

Bryan Cave LLP

David Zetoony, Partner | Jena Valdetero, Partner

BRYAN CAVE

bryancave.com | A Global Law Firm

TABLE OF CONTENTS

ABOUT THE AUTHORS i
INTRODUCTION 1
I. UNDERSTANDING THE NATURE AND SCOPE OF DATA EVENTS, INCIDENTS, AND BREACHES 3
A. Security Events 3
B. Security Incidents 3
C. Security Breaches 4
II. DATA SECURITY INCIDENT READINESS 7
A. Cyber-Insurance 8
B. Written Information Security Program 14
C. Incident Response Plans 15
D. Security Representations to Employees 17
E. Agreements with Service Providers 18
F. Identity Theft Services 21
G. Whistleblower Policies 24
H. Practicing For a Data Breach 25
III. INCIDENT RESPONSE 27
A. Investigating a Security Incident 27
1. Include Legal Counsel at the Inception of an Investigation 27
2. Form a Core Team to Respond to a Breach 28
3. Preserving Evidence 29
4. Retaining a Third-Party Forensic Investigator 31
5. Assigning a Crisis Manager 32
6. Investigating Employees 34
7. Responding to Employee Misconduct 35
8. Responding to Whistleblowers 35
B. Coordinating with Service Providers 36
C. Communicating with Law Enforcement 36
D. Communicating with Impacted Employees 37

1. Do State Laws Apply to Your Organization? 38
2. What Personally Identifiable Information Triggers Notification? 38
3. How Quickly Must You Notify Affected Employees? 39
4. What Information Does the Notice Have to Include? 39
5. How Must an Organization Notify Affected Employees? 40
6. Should an Organization Ever Voluntarily Notify Employees of a Breach? 41
7. Is Notification Required To Any Other Parties? 41
E Unique Issues Relating to Specific Types of Breaches 42
1. Lost Laptops and USBs 42
2. Errant Emails 42
3. Tossed Files 43
4. Tax/W-2 Breaches 44
5. Unauthorized Authentication to Service Provider Accounts 45
6. Breaches Involving Health Information 46
CONCLUSION 47

ABOUT THE AUTHORS

Jena Valdetero is a partner at Bryan Cave LLP where she serves as the co-leader of Bryan Cave LLP's data breach response team. She has provided counseling to dozens of clients in connection with data privacy and security issues. She is a Certified Information Privacy Professional, U.S. (CIPP/US), by the leading privacy trade organization, the International Association of Privacy Professionals. In addition to her privacy practice, Ms. Valdetero handles litigation matters on behalf of a variety of clients, including class action litigation, in both state and federal courts.

David Zetoony is a partner at Bryan Cave LLP and the leader of the firm's international data privacy and security practice, and the co-leader of Bryan Cave's data breach response team. Mr. Zetoony has helped hundreds of clients respond to data security incidents, and, where necessary has defended inquiries concerning the data security practices of corporations. He is the author of leading handbooks on data security including Data Privacy and Security: A Practical Guide for In-House Counsel and the Better Business Bureau's Data Security Made Simpler. He represents clients from a variety of industries ranging from national department stores to international outsourcers.

Special thanks to Christopher Achatz, Joshua James, and Jay Warren for contributing to sections of the Handbook.

INTRODUCTION

About twelve years ago, when most people had never heard the term "data breach", a colleague asked me what type of law I practiced. I tried to explain that I helped companies collect, secure, and share data, and, when data was inadvertently lost or breached, I helped them take steps to minimize any adverse impact. He thought for a while and said "what types of companies need to be worried about a data breach?" He was surprised when I looked him in the eye and said *every* company needs to be concerned about a data breach.

The reason was simple. Every company, whether its mission is manufacturing, sales, service, retail, or software, has employees and, if you have employees, then you have extremely sensitive personal information in your possession – *e.g.,* Social Security numbers, direct deposit numbers, tax forms, passport information, health information, etc.

Since then, the world has changed. One of the largest department stores lost information relating to nearly one third of the United States population in a month; one of the largest health care providers lost information relating to another quarter of our population; major political parties have been hacked; so, too, have our federal and state governments.

When you examine the hundreds of data breaches and thousands of data security incidents that occur each year, a large number of them still involve human resource-related issues. This includes situations in which human resource data was inadvertently lost or was wrongfully acquired by a third-party hacker or, in a small number of cases, a current or former employee maliciously stole or released information.

Since the first publication of our data breach handbook in 2014, the legal ramifications for mishandling a data security incident have become more severe. In the United States, the number of federal and state laws that claim to regulate data security has mushroomed. The European Union has also enacted a new General Data Protection Regulation which will extend the United States framework for responding to data breaches across the EU, but with significantly enhanced penalties. The EU's version of data breach notifications might best be characterized as US law on steroids and will be sure to cause more sleepless nights on the other side of the Atlantic.

In order to effectively respond to a data security incident, human resource professionals and labor and employment attorneys must understand what a "security incident" entails, what their organization should do to prepare itself before an incident occurs, and what practical considerations will confront the organization when an incident arises. Effective response also requires understanding and preparing for the possibility that a data security incident may lead to lawsuits, regulatory investigations, or public scrutiny.

This handbook provides a basic framework to assist human resource professionals and labor and employment attorneys with handling a security incident. Section I explains what security incidents are, how often they occur, and which types of organizations are most at risk. It also discusses the costs that a security breach may impose on an organization. Section II outlines how human resource professionals can help their organization prepare for a security incident.

Section III walks through the different steps that must be taken once a security incident occurs, including how to investigate the incident and how to communicate with other entities, such as business partners or law enforcement. It also discusses steps to consider if the security incident is, in fact, a "breach" that might harm employees.

I hope that this handbook provides a valuable resource to human resource professionals, as they continue to form part of the front-line in responding to data breaches.

David A. Zetoony
September 2017

I.
UNDERSTANDING THE NATURE AND SCOPE OF DATA EVENTS, INCIDENTS, AND BREACHES

Many human resource professionals may not be familiar with data security-related terminology. As a result, when an incident occurs there can be confusion when terms like "security event" or "data breach" are thrown around. Indeed, one of the most common mistakes made by human resource professionals is *assuming* that a situation involves a data breach because that term is used by others, and then believing that statutory or contractually obligations that are triggered by a breach must apply.

The problem stems from the fact that many people refer to a "data breach" loosely as any situation in which data may have been removed from, or been lost by, an organization. Technically, however, "data breach" is a legally defined term that typically refers in the United States to a –situation where there is evidence of an unauthorized "acquisition" or "access" to certain types of sensitive personal information (*e.g.,* Social Security Numbers, driver's license numbers, or financial account numbers) that trigger a legal obligation by an organization to investigate the situation and to notify employees, consumers, regulators, or business partners. It is important to realize that many of the situations that are referred to as "data breaches" in the media, and possibly by others in your organization, do not in fact meet the *legal* definition of the term. For the purpose of clarity, this handbook uses three terms to refer to security situations: a data security "event," "incident," and "breach."

A. Security Events

A "security event" refers to an attempt to obtain data from an organization or to a situation in which data might be exposed. Many security events do not necessarily place the organization's data at significant risk of exposure. Although an event might be serious and turn into an "incident" or a "breach," many events are automatically identified and resolved without requiring any sort of manual intervention or investigation and without the need for legal counsel. For example, a failed log-in that suspends an account, a phishing email that is caught in a spam filter, or an attachment that is screened and quarantined by an antivirus program, are all examples of security events that happen every day and typically do not lead to an incident or breach.

B. Security Incidents

A "security incident" refers to an event for which there is a greater likelihood that data has left, or will leave, your organization, but uncertainty remains about whether unauthorized acquisition or access has occurred. For example, if you know that an employee has lost a laptop, but you do not know what information was on the laptop or whether it has fallen into the hands of someone who might have an interest in misusing data, the situation would be referred to as a "security incident." Another way to think of a security incident is as a situation in which you

believe that electronic data that contains personal information *may* have been improperly accessed or acquired.[1] As discussed in this handbook, security incidents almost always necessitate that you thoroughly investigate to determine whether personal information was improperly accessed or acquired. Put differently, companies conduct investigations to determine whether there is, or is not, evidence that would redefine the "incident" as a "breach."

Security incidents are attributable to a variety of different causes—sometimes referred to as "attack vectors." Approximately 75% are caused by third parties, with 25% relating to the actions of employees from within an organization.[2]

C. Security Breaches

As discussed above, a "security breach" or a "data breach" is a legally defined term. The definition varies depending upon the data breach notification law that is at issue. As a general matter, however, a security breach refers to a subset of security incidents where the organization discovers that sensitive information has been accessed or acquired by an unauthorized party and that acquisition has created the possibility that an employee or a consumer might be harmed by the disclosure. In the laptop example provided above, if you determine that the laptop was stolen and it contained unencrypted Social Security numbers (*e.g.,* a spreadsheet of employee W2 information), the incident would fall under the definition of a "security breach." As discussed below, security breaches almost always dictate that you consider the legal requirements of data breach laws.

If you identify a security breach, you should be cognizant that security breaches typically impact organizations in a number of ways:

> Reputational Cost: A security breach can erode the confidence of employees, customers, donors, or clients, which can significantly impact sales, recruitment, and/or the overall reputation of your organization. Often the indirect cost to the organization from adverse publicity significantly outweighs direct costs and potential legal liabilities.
>
> Business Continuity Cost: Breaches that create, expose, or exploit vulnerabilities in network infrastructure may require that a network be taken off-line to prevent further data-loss. For organizations that rely heavily on IT infrastructure (*e.g.,* an ecommerce retailer), removing or decommissioning an affected system may have a direct adverse impact on the organization.

---

[1] David Zetoony, ed., Council Of Better Business Bureaus, Data Security Guide: Data Security – Made Simpler: Common Technical and Legal Terms – A Glossary, *available at* http://www.bbb.org/council/data-security-made-simpler/common-technical-and-legal-terms/

[2] *See, e.g.*, Verizon 2017 Data Breach Investigation Report *available at* http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf (last viewed June 17, 2017).

Competitive Disadvantage: Breaches that involve competitively sensitive information such as employment compensation, trade secrets, customer lists, or marketing plans may threaten the ability of your organization to compete.

Investigation Costs: Security incidents involving IT infrastructure may require the services of a computer forensics expert in order to help investigate whether a breach has occurred and, if so, the extent of the breach. Security incidents that involve the potential of insider misconduct may necessitate an internal investigation in order to determine whether an employee has committed misconduct.

Contractual Costs: Your organization may be contractually liable to business partners in the event of a data security breach. For example, a breach involving a retailer's electronic payment system will typically trigger obligations under the retailer's agreements with its merchant bank and/or its payment processor. Those obligations may include, among other things, the assessment of significant financial penalties. As another example, some outsourcing contracts require companies that provide services to other companies to pay for the cost to notify impacted individuals and to indemnify their business partner from lawsuits. In the human resource context, if your organization is a human resource-related service provider, a breach of information that has been placed in your custody in order to provide services could lead to contractual liabilities depending upon the terms of your service agreement.

Notification Costs: If your organization is required to, or voluntarily decides to, notify employees of a data security incident, it may incur direct notification costs relating to identifying applicable data breach notification statutes and physically printing and mailing notification letters. Although most statutes do not require organizations to provide employees with credit monitoring, identity−theft insurance, or identity−theft restoration services, in some situations, offering such services at the organization's own cost has become an industry standard practice.

Regulatory Costs: A regulatory agency may decide to investigate whether an organization should have prevented a breach and/or whether an organization properly investigated and responded to it. In addition, some regulatory agencies are empowered to impose civil penalties or monetary fines in the event that they determine the organization's security practices were deficient or that an organization failed to properly notify employees, consumers, or the agency itself in a timely matter. Significant legal expenses can be associated with a regulatory investigation.

Litigation Costs: While Bryan Cave LLP's 2016 Data Breach Litigation Report found that approximately 5% of publicly reported data security breaches result in the filing of a federal putative class action lawsuit,[3] the vast majority of suits filed did not relate to breaches involving the loss of human resource-related data; far fewer HR-related data breaches turn into litigation.[3] Although most suits have not resulted in a

[3] Zetoony, David, Jena Valdetero, and Joy L. Anderson. 2016 Data Breach Litigation Report (April 6, 2016).

finding of liability, defense costs and settlement costs can be significant if litigation is initiated.

TIP:	While it may seem like there is no harm in using terms like "data breach" to describe any event or incident, the term can cause confusion to employees, others in your organization, or the public who may jump to the conclusion that you have actually confirmed that sensitive information has been accessed or acquired by a bad actor. Using the correct terminology can avoid that problem.

II.
DATA SECURITY
INCIDENT READINESS

Many human resource departments, legal departments, and information technology professionals have relied on the adage that the best way to prepare for a data security incident is to prevent one from happening in the first place. As a result, the historical focus for many organizations has been on taking steps to protect data and to prevent a breach from occurring. Such steps include instituting written information security programs that describe the security infrastructure of an organization, investing in defensive information technology resources, installing monitoring systems, and training employees on good security practices.

Most organizations now realize that even the best security cannot prevent a data breach. For example, the number of attacks from third parties that exploit previously unknown software vulnerabilities (sometimes referred to as "zero-day exploits") has risen dramatically. More importantly, however, the majority of data breaches involve human behavior. Although employees can be trained to practice good data security habits, when employees are involved the possibility of accidental loss of information can never be completely eliminated. For example, one of the oldest and most successful attack vectors involves "phishing." Phishing is essentially lying to an employee – typically by impersonating someone of importance, like the company CEO – in an attempt to get the employee to inadvertently contribute to a data breach. There are hundreds of variants of phishing attacks that range from having employees click on attachments in email that cause malware to be downloaded into a company's network to impersonating senior management and instructing employees to wire funds outside of the organization. The new rule of thumb is that it is not a matter of *if*, but rather *when*, a security breach will occur. From that vantage point preparing in advance for how your organization will respond when a security incident or breach occurs is essential.

Data security incident readiness is a process that involves human resources, management, information technology, public relations, and legal. It typically includes the creation of a plan for how an organization will respond to an incident and/or a breach, as well as continual cross-staff and cross-department training to teach personnel about the plan and how to implement it. Each training exercise inevitably identifies areas in which an organization can improve its plan and/or provide additional training to improve its response.

In addition to supporting the organization's planning and training efforts, human resource personnel have a special role in terms of data security incident preparation. When a security breach occurs, the response to the breach often involves interactions with employees. This may include investigating whether employees were involved in causing a breach, or communicating to employees that their information may have been compromised. To that end, human resource professionals should review their organization's incident response plan to make sure that they understand what to do if a breach occurs. They should also be familiar with some of the core documents that come into play when investigating a security incident. The remainder of this chapter provides a description of these documents and what human resource professionals should

consider in order to evaluate and understand their role in the organization's preparation for a possible breach.

A. Cyber-Insurance

Only about 50% of companies have purchased insurance specifically designed to cover part, or all, of the costs of a data security breach ("cyber-insurance").[4] In order to understand why some companies choose to purchase cyber-insurance, while other companies choose not to, you have to take a look at what cyber-insurance in general is designed to do, and whether a specific policy that your organization has (or is considering) truly mitigates risk for your organization.

Cyber-insurance policies differ dramatically in terms of what they cover, what they exclude, and the amount of retentions (*i.e.*, the amount of money that the insured organization is responsible for paying before the policy provides reimbursement). If your organization has a cyber-insurance policy, you should review it carefully before a security incident occurs so that you understand the degree to which the policy protects (or does not protect) your organization from potential HR incident-related costs and liabilities. If you are not used to reading an insurance policy, or are not familiar with cyber-related risks, consider asking others within your organization who may have more experience with interpreting insurance policies to review the policy with you. In some cases this may be your risk manager, your legal department, or your organization's outside counsel. Policies may also obligate your organization to take specific actions, such as notifying the insurer or using pre-approved data incident response resources (*e.g.*, investigators, credit monitoring, mailing services, public relations firms, or outside counsel). Because data security law is rapidly evolving and changing, you should try to review the policy annually to ensure that its protections continue to align with changes in the legal landscape, coverage trends, and your organization's operations.

The following checklist provides a guide to evaluating a cyber-insurance policy in connection with how it might apply to a HR data-related incident. The points to consider are broken down by type of issue/service for which you might seek insurance reimbursement or guidance. Before completing the checklist, it is important to determine whether your organization's goal in purchasing insurance is to help it handle typical data security incidents, to help it cope with catastrophic data security breaches, or both.

Forensic Investigators

- ❑ **Coverage**: Does the policy cover the cost of retaining a forensic investigator? Restrictions on which forensic investigators can be used can be important. Forensic investigation is not a commodity, and there can be significant differences between

[4] "Why 27% of US Firms Have No Plans to Buy Cyber Insurance," Insurance Journal (May 31, 2017) *available at* http://www.insurancejournal.com/news/national/2017/05/31/452647.htm.

investigators. While some insurance companies may focus on unit price (*e.g*. billable rates) when selecting the panel of providers that they prefer, many organizations prefer to focus on overall price, reputation, or the ability of an investigator to work well with the organization's HR, IT, or legal departments.

- **Sub-limit**: Does the policy have a sub-limit for forensic investigation costs? A sub-limit refers to a cap on the amount of money that the insurer is willing to pay, which may be less than the policy's overall limit. Is the sub-limit proportionate to the average cost of retaining a forensic consultant to investigate a data security incident?

- **Sub-Retention**: Does the policy have a sub-retention when hiring an investigator (*i.e.*, a deductible)? A sub-retention refers to the amount that your organization must pay before insurance will begin reimbursing you. In the context of HR-related data security incidents, the amount of the sub-retention may be the most significant factor when considering whether cyber-insurance is likely to help defray the cost of a forensic investigation. While the costs incurred by a forensic investigator can vary greatly, the highest cost investigations are often in situations in which the investigator must investigate hundreds (or sometimes thousands) of computer systems. Those types of investigations are *extremely rare* in the context of HR-related incidents where incidents often involve a single file, a single computer, or a single server. As a result, if there is a significant retention that must be met before the cost of a forensic investigator will be covered by the insurer, the insurance may have limited benefit. Indeed, sometimes a cyber-insurance policy can do more harm than good. For small incidents that will more than likely be below your retention, the organization may feel compelled to retain the insurer's choice for a forensic investigator while there is an extremely small likelihood that the insurer will cover any of the costs. In some situations, this means that the insurer gets to make the decision about which vendors your organization hires, but you have to bear the cost and consequences of their work performance.

Employee Notifications

- **Coverage**: Does the policy cover the cost of issuing notices to employees? If so, does the coverage give the organization the right to control how those notices are provided (*e.g.*, in paper format versus in electronic format)? Does it require that the organization avail itself of "substitute notice" when permitted by statute? Substitute notice refers to a process, permitted by most states, where an organization can publicize a breach via its website and/or state-wide media. If you make a substitute notice, you may not be required to send individualized letters to impacted employees. Many organizations – particularly in situations in which a breach involves only HR-related data – prefer not to publicize an incident (which may impact the overall reputation of the organization and result in clients or consumers mistakenly believing that their data was impacted). As a result, it is important to make sure that your insurer cannot refuse to pay for printing and

mailing notification letters if your organization decides that issuing notifications in that manner is necessary to help protect the organization's reputation and brand.

- **Exclusions**: Does the policy exclude notifications that are not expressly required under a state data breach notification statute (*e.g.,* "voluntary" notifications)? If so, are there situations in which your organization might decide to issue voluntary notices in order to limit reputational damage or decrease the likelihood of a class action filing? Make sure that you understand if these notices will not be covered under the policy.

- **Sub-limit**: Does the policy have a sub-limit for the total cost of issuing employee notifications or the total number of employee notices for which the policy will provide reimbursement? If so, is the sub-limit proportionate to the quantity of employees about whom the organization maintains personal information?

- **Sub-retention**: Does the policy have a sub-retention (*i.e.*, a deductible) for either the cost of issuing employee notifications, or the number of employee notices that must be paid for by the organization before insurance coverage kicks in? In the context of HR-related data security incidents the amount of the sub-retention may be the most significant factor to look for when considering whether cyber-insurance is likely to provide a benefit. Specifically, organizations that have fewer than 5,000 employees often find that even if they had an incident that resulted in the loss of all of their current and former employees, notification costs still fall below the retention and, therefore, insurance provides little, if any, benefit.

Identity Theft Services

- **Coverage**: There are a number of different services that employers consider offering to employees following a data breach that involves employee data. These include credit monitoring (*i.e.,* monitoring employees' credit reports for suspicious activity), identity restoration services (*i.e.,* helping employees restore their credit or helping employees close fraudulently opened accounts), identity-theft insurance (*i.e.,* defending employees if creditors attempt to collect upon fraudulently opened accounts and reimbursing employees for any lost funds), and dark web monitoring (*i.e.,* monitoring the internet and hacker-websites to see if they refer to your employees). For simplicity, we refer to all of these services collectively as "identity theft services." The first thing to check is whether the cyber-insurance policy offers some, or all, identity theft services in the event of a breach. If so, look for any limitations on when the coverage is triggered.

- **Exclusions**: Some policies exclude identity theft services if providing them is not "required" by law. If your policy contains this exclusion, it is important to note that very few laws formally require that employers offer identity theft services. As a result, consider whether a policy that requires that such a law be triggered is providing anything of real value.

- **Panel providers**: Does the policy require you to use a certain company to provide identity theft services? If so, do you have a relationship with a different provider? Does the provider that is listed on the panel have a history of consumer complaints? Does it have a history of alleged unfair or deceptive trade practices? Must the provider, or the insurer, indemnify you if one of your employees complains about the services offered? It's important to note that different insurance companies select different panel providers for different reasons, and just because a company is listed on your insurance company's panel does not necessarily mean that it is the right choice for your organization. For example, some panel providers do not offer the full range of identity theft services. Other panel providers may have a financial interest in making sure that you purchase a particular identity theft service, even if that service is not the best "match" to the type of incident that impacted your employees.

- **Sub-limit**: Does the policy have a sub-limit for the total cost that it provides for identity theft services? If so, is the sub-limit proportionate to the quantity of employees (and former employees) about whom you have information?

- **Sub-retention**: Does the policy have a sub-retention (*i.e.*, a deductible)? Be wary of insurance policies with significant retentions. You may find yourself having to pay an identity theft service provider that you did not choose, at a rate that you did not negotiate, for services that you might not have selected.

- **Cost Reductions**: Organizations that have fewer than 5,000 employees often find that, even if they had an incident that resulted in the loss of all of their current and former employees' data, the cost of identity theft services is still below the retention and, therefore, insurance provides little, if any, direct benefit. Even if insurance provides no financial coverage, in some situations it may provide an indirect benefit. The retail cost of identity theft services is often exponentially greater than the wholesale cost. However, many identity theft service providers charge fixed minimum amounts (*e.g.*, $10,000) in order to access that wholesale rate. As a result, in a small breach, you may find that it costs the same to offer an identity theft service to 100 employees as it would to offer it to 1,000 employees. Some identity theft service providers may waive that fixed fee for companies that have insurance via one of the provider's partners. As a result, even if the retention is set so that your insurance does not cover the cost of identity theft services, you may be able to save money if a fixed fee or start-up fee is waived.

- **Pre-Paid Fees**: Many employers now provide their employees with identity theft-related services as part of an employee benefits package. If your organization pre-emptively purchased identity theft services for all of your employees, or purchased the right to provide employees with identity theft services if an incident arises, many insurance companies may refuse to compensate you for those costs by claiming that the fees and expenses that were incurred by your company were part of its normal course of business. As a result, if you already provide these types of benefits and are evaluating the utility of

a cyber-insurance policy, you should consider whether coverage for identity theft services has any value to you.

Regulatory Proceedings

- **Coverage**: Does the policy cover regulatory proceedings that may result from a breach? If so, does the coverage extend to legal fees incurred in a regulatory investigation or regulatory proceeding? Does it also cover the fines or civil penalties that may be assessed as a result of a proceeding?

- **Exclusions**: Does the policy exclude investigations brought by agencies that are likely to investigate your organization? For example, most employers are subject to the jurisdiction of the Federal Trade Commission and their state attorney general when it comes to how they protect their employees' data. If your policy excludes such investigations, it may be of relatively little value. If you offer a self-funded health insurance plan, you should avoid any policy that excludes coverage for investigations brought by the Department of Health and Human Services.

- **Sub-limit**: Is the sub-limit proportionate to the average cost of defending a regulatory investigation and/or the average cost of the fines assessed to other organizations in your industry?

- **Sub-Retention**: Does the policy have a sub-retention (*i.e.*, deductible) for the cost of a regulatory investigation? If so, is the sub-retention well below the average cost of regulatory penalties and fines? If legal fees incurred in a regulatory investigation are covered, is the sub-limit well below the legal fees that you would expect?

Service Provider Incidents

- **Coverage**: Most companies provide employee-related data to health insurance providers, third-party administrators, payroll processors, tax preparers, and/or disability insurers. Some, but not all, insurance policies are drafted to cover security incidents that impact data that is in your possession, or is in the possession of one of your service providers.

- **Exclusions**: If your policy does not state that it covers your employees' data while in the possession of a service provider, confirm whether the policy excludes data security incidents that occur to third parties holding your employees' data. Some policies don't include an express exclusion, but when you look at the definitions of "personal information," "security systems" or "information technology," it makes clear that the policy only applies to data that is physically under your organization's control.

- **Responsibilities**: Although some policies do not expressly state that they cover breaches that occur while data resides with your service provider, they are triggered anytime your organization has a statutory duty to investigate or respond to a security incident. Most

state data breach notification statutes require that the "owner" of data issue data breach notifications and that a licensee of data only notify the owner. Because most employers are the "owners" of the data that they collect about their employees, if a service provider informs you of a data incident, you may be able to trigger your insurance coverage based upon your statutory obligation to investigate the incident and to notify the employee and/or government agencies.

Legal Assistance

- **Coverage**: Does the policy permit you to retain an attorney to help (1) investigate and document an incident, (2) retain a forensic investigator if needed, (3) review contracts with service providers, (4) identify statutory obligations to notify employees and regulators, and (5) advise on steps that may reduce the likelihood of a class action or a regulatory investigation? Does the policy cover legal expenses incurred in defending all types of claims?

- **Exclusions**: Does the policy exclude coverage for lawyers to provide assistance concerning some aspect of a security breach response? For example, some insurance policies will not pay for your attorney to negotiate or settle contractual claims or for your attorney to deal with government regulators. Other insurance policies exclude coverage for lawsuits that assert legal theories that are common in class actions (*e.g.* consumer fraud, deceptive practices, or unfairness claims). Finally, if your in-house attorney helps you manage a security incident, most insurance policies will not reimburse you for their time and costs, but will reimburse you if you use outside counsel.

- **Panel providers**: Does the policy require that you use a specific law firm(s) or does it allow you to select your own attorneys? Do you have relationships with any of the firms that are on the panel? If not, have you done due diligence concerning each firm's experience handling data security breaches? For example, you should consider whether the law firms that you are being offered have taken legal positions that might benefit the insurer, but would not benefit your ability to obtain coverage under your policy. You want to make sure that you feel confident that your counsel will provide independent advice, even if that advice may not be in the insurer's interest. You may also want to make sure that the volume of work that the attorney receives from the insurer will not cause the attorney to hesitate to give you advice that the insurer might not like.

TIP: Cyber-insurance is not right for every employer. While a good cyber-insurance policy may help defray some of the costs of a data breach or protect an organization from third-party lawsuits, a bad cyber-insurance policy can provide a false sense of security, erode your organization's autonomy, and divert money that might be better spent improving the security of your organization through technology or employee training.

B. Written Information Security Program

After a security breach occurs employees, the media, and regulators often ask what measures a company took to try to prevent the breach in the first place. HR professionals should consider, therefore, whether their organization would be able to produce documents that demonstrate that it was attempting to secure sensitive information. Many outside observers will expect that this includes, at a minimum, a written information security program or "WISP." Rhode Island and Massachusetts require employers to implement and maintain WISPs if they control sensitive categories of personal information such as employee Social Security numbers about residents of those states. Even if the laws of all 50 states do not legally require a company to have a WISP, regulators will likely inquire about whether the company has one if they become aware of a breach of employee personally identifiable information or "PII".

The format and contents of a WISP depend greatly on the number of employees about whom you have information (and, therefore, the total quantity of information that is in your organization's possession). Put differently, the WISP of a five employee non-profit typically looks very different than the WISP of a multinational company with tens of thousands of employees. Nonetheless, there are areas of commonality. A well-written WISP usually describes the following:

- The administrative, technical, and physical safeguards that exist to keep sensitive personal information secure
- The process used by the organization to identify, on a periodic basis, internal and external risks to the information that it maintains
- The specific employee who is ultimately responsible for maintaining and implementing security policies
- The sensitive information maintained by your organization
- Where and how sensitive information will be stored within your organization
- How sensitive information can be transported away from your organization

- Procedures for:
  - Username assignment
  - Password assignment
  - Encryption format
  - Provisioning of user credentials
  - De-provisioning of user credentials (*e.g.*, for taking away the ability of terminated employees to log into your network)
  - Employee training on security topics
  - Destroying data
  - Retaining service providers that will have access to data

Companies that maintain sensitive information about individuals other than their employees may choose to base their WISP upon standards or formats created by third parties. Although there are many frameworks that can be looked to, some of the most popular frameworks are those published by the International Standards Organization ("ISO") and the National Institute for Standards and Technology ("NIST"). Organizations that adopt one of these standards to describe how they protect consumer data typically fold the security practices that surround employee-data into their larger security framework.

> TIP: For some organizations, a written information security program is a complex document that may include hundreds of sections. For others, a written information security program can be a simple document that endeavors to memorialize what your company is doing to protect employee data. If you do not already have a written plan, do not allow the perfect to be the enemy of the good. Keep it simple and focus on the main topics that others would expect to be included.

C. Incident Response Plans

An incident response plan explains how an organization handles security events, security incidents, and security breaches. Among other things, the plan helps employees from different departments understand the role that they are expected to play when investigating a security incident and identifies other people within the organization with whom they should be coordinating. The plan can also help educate employees concerning what they should do (and should not do) when faced with a security incident and can provide them with a reference guide for resources that may help them effectively respond to a breach.

Incident response plans take a variety of forms, and there is no mandated structure. The following topical recommendations, however, may help you draft an incident response plan or evaluate the thoroughness of one that already exists:

- **Definition of Security Event, Incident, and Breach**. Consider explaining the difference between an event, incident, and breach so that those in the organization involved with incident response understand the distinction.

- **Security Event Escalation**. By their very nature, security events are relatively common occurrences. Only a small percentage of events will become incidents, and an even smaller percentage of events will ultimately become breaches. Nonetheless, it is important to explain the process under which an event should be escalated to an incident or a breach and the impact that such an escalation has on who within the organization needs to become involved in an investigation and how the investigation should be handled.

- **Responsibilities For Conducting an Incident Investigation**. The plan should explain who within the organization is responsible for investigating security incidents, to whom information should be reported, and who has the authority (and responsibility) to seek additional resources when needed. To the extent that one of the purposes for conducting an investigation is to provide in-house or outside counsel with information needed to make legal recommendations, the plan should consider whether an organization desires the investigation to be conducted under the auspice of the attorney-client privilege and attorney work product doctrine. If so, the plan should make clear that the investigation is operating at the direction of counsel and should provide instructions to employees who may be collecting information on how to help preserve privilege.

- **Internal Contact Information**. Many plans include a quick reference guide naming the people within an organization who can help in the investigation of a security incident and their emergency contact information (*e.g.*, email address, home phone, and mobile phone).

- **External Contact Information**. Many plans include a quick reference guide naming the people outside of an organization who can help in the investigation of a security incident. That may include contacts with law enforcement (*e.g.*, FBI and Secret Service), outside counsel, forensic investigators, call center support, identity theft services, public relations experts, etc. If the organization has a cyber-insurance policy, you may want to list the approved vendors in the plan and the insurer's contact information to notify of a potential claim.

- **Recordkeeping**. Plans typically explain the types of documents and records that should be kept concerning the investigation in order to permit legal counsel to reconstruct, if necessary, when the organization knew certain pieces of information and when the organization took certain steps. Such reconstruction may be necessary in litigation or a

regulatory investigation. The plan should direct recordkeeping to be done by a designated person and caution against too many participants recording information, particularly when that information is subject to change or may not be accurate.

- **Post-Incident Reporting.** Many plans discuss how the organization will take information learned during an incident and incorporate that back into the organization's security program. This might include "lessons learned" from how an incident was handled or ways to prevent an incident from occurring again.

> TIP: Many organizations overthink their incident response plan and create a long, complex document that is of little use when a breach occurs. The best incident response plans are short and focus on practical information that the incident response team can quickly find and use in the event of a breach.

D. Security Representations to Employees

In 2005, Michigan became the first state to pass a statute requiring employers to create a privacy policy that explains to employees what the employer does with their Social Security numbers, and with whom the numbers are disclosed. Other states, such as New York, Connecticut, Massachusetts, and Texas, have adopted similar statutes. Although not required by law, many employers choose to include information on data security measures within employee privacy policies. If such policies are not drafted carefully, they can inadvertently impose obligations concerning the protection of employee information that are greater than those otherwise imposed by law. Conversely, employee privacy policies create an opportunity to help set employee expectations for how the employer will respond to a security incident, and what types of services the employee can expect from the employer in the event of a breach.

When drafting or reviewing an employee privacy policy you should consider the following implications on data security:

- Does the privacy policy guarantee that employee information will remain confidential in all situations? If so, it may create a standard that is impossible for the employer to meet.

- Does the privacy policy explain how employee Social Security numbers and other personal information are protected? If so, is the information provided accurate and precise?

- Does the privacy policy describe what disciplinary measures might be taken against employees who cause the inadvertent disclosure of sensitive personal information?

- ❑ Will the privacy policy be published in an employee handbook, procedures manual, or similar document? If not, will each employee be able to access the policy?

- ❑ Does the privacy policy use terms that might be misunderstood or misconstrued by a regulator or a plaintiff's attorney?

- ❑ Does the privacy policy discuss the different ways in which the employer may contact an employee if a security breach impacts the employee's information?

- ❑ Does the privacy policy explain that the employer may decide not to communicate with employees about a security incident until an investigation is complete in order to ensure that the information provided to employees is accurate and precise?

> TIP: If you have a website privacy policy, that policy may be written broadly enough to encompass the information that you collect about your employees. If it is, you may be able to avoid drafting a separate stand-alone employee specific policy.

E. Agreements with Service Providers

Almost every employer utilizes service providers. Some service providers require information about employees in order to provide the employee with human resource benefits (*e.g.*, health insurance, vision insurance, dental insurance, disability insurance, life insurance, parking, etc.). For example, in order for a health provider to send benefits information to a new employee, they must know the name of the employee, what premium should be charged, the employee's health insurance elections, and the employee's beneficiaries who will also be covered under the policy. Other service providers require information about employees in order to help employers manage the employment relationship (*e.g.*, payroll processing, tax processing, benefits processing, disability processing etc.). For example, a tax preparer needs access to each employee's Social Security number, salary, and address in order to prepare, and/or submit W-2 forms for an employer.

As with any company, service providers cannot guarantee that the information provided to them will remain secure in all situations. While a guarantee may be impossible, employers have a vested interest in making sure that their service providers utilize reasonable security measures to help prevent the loss of data, and in understanding how their service providers will react in the event of a security incident. Employers should consider the following factors when reviewing a contract with a service provider:

- ❑ **Security standard**. A service provider that receives sensitive information concerning your employees should contractually represent and warrant that they are not only in compliance with law, but that they take reasonable and appropriate security measures to

protect your employees' information. If your organization has specific standards for the security protocols that it applies, consider integrating those standards into your agreement with the service provider. You may also wish to negotiate the right to audit the security practices of the service provider.

- **Notification of a suspected data breach.** If a data breach occurs that involves sensitive categories of information, states typically require that a service provider notify the data owner. State notification laws, however, often give a service provider flexibility to conduct an investigation of the security breach to understand its scope before putting you on notice. Many employers negotiate data breach notification provisions that exceed statutory requirements by forcing service providers to notify them when the service provider first suspects a data breach and not wait until after the service provider has completed an investigation and conclusively determined that a breach occurred.

- **Notification of other suspected data security incidents**. As discussed above, "data breach" is a legally defined term that typically refers to unauthorized access or acquisition of certain fields of sensitive information. Service providers often experience security incidents that, upon investigation are not, in fact, data breaches. For example, service providers that permit your employees to establish a user name and/or password in order to log into an online portal often monitor employee accounts for indications that an unauthorized person has obtained an employee's username and/or password and attempted to log in. Depending upon what the attacker views once they have logged in, the incident may not qualify as a "data breach." Specifically, the service provider's network itself has not been compromised by the unauthorized login of authorized user credentials and, while the attacker may have viewed nonpublic information about an employee that information may not trigger a breach notification statute (*e.g.*, if the information contained only the employee's salary, or contained data elements that the attacker possessed prior to viewing the account). While this type of "unauthorized authentication" may not be the fault of your service provider, you may have an interest in having the service provider alert you of the situation so that you can advise an impacted employee that a third party appears to have access to their account credentials (*e.g.*, user name and password) and may have accessed their information.

- **Liability**. The degree to which a vendor can, or should, be held liable for a data breach varies greatly. If the breach was caused by a third party (*e.g.*, a criminal attacker), the service provider may not have been able to prevent the breach and, as a result, justifiably may feel that it should not be liable. Conversely, even when a breach was caused by a third party, between the employer and the service provider, the service provider may have had a greater opportunity to protect the data from attackers. As a result, an employer may justifiably feel that it should not be liable. The net result is that there are often reasonable arguments for, and against, assigning responsibility to a service provider when the service provider's system was breached by a third party. In any case, it is important that employers understand the amount of liability that your vendors share in connection with a

security incident and, if necessary, renegotiate your agreements to include industry-reasonable terms.

- **Remediation of security vulnerabilities**. The adage of "it's not if, but when" applies to vendors just as it does to employers. As a result when establishing a vendor relationship, or negotiating a contract with a vendor, you should anticipate that a security failure will occur and plan what the parties' respective obligations will be in such eventuality. Part of that discussion should include what obligations the vendor will have to remediate security failures that are identified as part of a breach. While some security failures are relatively easy to fix on a going forward basis (*e.g.*, patching a terminal that had an out-of-date operating system, or updating the malware signatures to an anti-virus program), other security failures may be more complex and even a diligent vendor may not be able to provide an immediate fix (*e.g.*, redesigning a database, applying different at-rest encryption technologies, etc.). As a result, it may be difficult, if not impossible, for a vendor to warrant before a breach happens and a security vulnerability is identified that any and all vulnerabilities will be fixed – let alone provide a precise timetable for how long remediation may take. When searching for a middle ground some employers require that a vendor take "commercially reasonable" steps to remediate significant security vulnerabilities. Other employers draft their service agreement to allow them to terminate a relationship with a vendor for-cause if the vendor will not, or cannot, remediate a security vulnerability.

- **Termination rights**. Employers should remember to continually reevaluate throughout the vendor relationship whether the level of security that a vendor can offer matches the level of security required by the employer. If, at some point, there is a mismatch between an employer's needs and a vendor's capabilities, the employer may want the ability to terminate the vendor relationship without incurring penalties and transfer its data to a new provider.

- **Insurance**. If the agreement that you have with a service provider imposes obligations upon them in the event of a data breach (*e.g.*, to issue notifications to employees, to provide identity theft related services to your employees, or to defend and indemnify your organization), it is important to consider whether the service provider would have the financial ability to meet these obligations in the event of a breach. When thinking about a service provider's financial capacity, remember that if a service provider experiences a network breach that impacts the information of some (or all) of their clients they may be liable to dozens, hundreds, or even thousands of companies – not just your organization. If you have doubts concerning their financial strength to absorb the impact of a data breach consider requiring that they maintain cyber-insurance and that your organization be identified as an insured on their policy.

TIP: A service provider that is willing to "guarantee" that your employees' information will always be secure, or that represents that they have never had a data security breach, may be demonstrating a lack of data security-related maturity. In such cases, while a contractual guarantee is beneficial if a breach occurs, the service provider may be unwilling (or unable) to comply with their contractual commitments.

F. Identity Theft Services

There are a number of different services that employers consider offering to employees following a breach of employee data. Many employers don't fully understand the difference between identity theft service offerings. Unfortunately, the fact that different service providers use different terms to describe identity theft services and products, and the existence of misinformation in the marketplace (sometimes produced by industry members that have a vested interest in selling one type of product over another), makes it difficult for many employers to educate themselves about what options exist and which products or services may be the most appropriate to offer in a particular situation. The net result is that too many employers inadvertently jump to the conclusion that one type of product – like credit monitoring – should be offered in connection with every type of data breach. The following provides a summary of each of the main types of identity theft services:

Credit report. A "credit report" is a report generated by a credit reporting agency (*e.g.*, Equifax, Experian, or Transunion) that summarizes information maintained by those companies about an employee. That information typically includes where the employee lives, how often the employee pays his or her bills, whether the employee has been sued, and which financial institutions have accounts related to the employee. An employee can review their credit report to determine if all financial accounts that have been opened in the employee's name are valid. By law, an employee has a right to obtain a credit report from each of the credit reporting agencies at no cost at least once a year by either visiting annualcreditreport.com or contacting the credit reporting agencies directly. As a result, some employers decide that it is not necessary to pay a third party to provide their employees with a credit report when the report itself is most likely free to the employee.

Credit monitoring. While a credit report provides information about financial accounts that were opened in the past using the employee's name, it does not help the employee determine if a bad actor uses the employee's information to open a financial account after the credit report is run. "Credit monitoring" refers to a service where a third party monitors the employee's credit report for any indication that a new financial account has been created. If an account is created, the credit monitoring company notifies the employee and asks the employee to determine whether the new account is legitimate (*i.e.*, created by the employee) or fraudulent (*i.e.*, the result of identity theft). There are a number of different companies – including the credit reporting agencies themselves – that

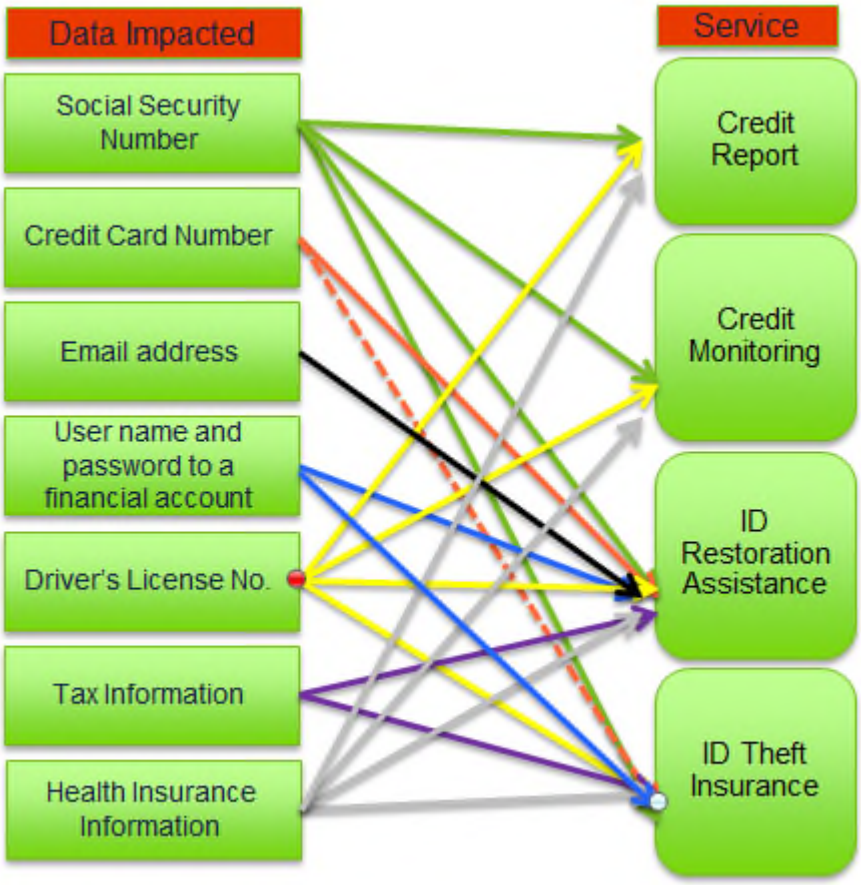
offer credit monitoring services. If an employer decides to offer credit monitoring to employees they typically must select whether the monitoring will look at a single credit reporting agency (*e.g.*, Equifax) or all of the main credit reporting agencies (*e.g.*, Equifax, Experian, and Transunion). The former service is typically referred to as "single bureau" monitoring; the latter is typically referred to as "triple bureau" monitoring.

Identity restoration services. "Identity theft restoration services" describe resources that are offered by third parties to assist employees with rectifying a fraudulently opened account or other forms of identity theft (*e.g.*, fraudulent tax filings under the employee's name). That assistance might include a case manager or consultant who the employee can call to understand the implications of a fraudulently opened account. The case manager can provide direction and guidance to the employee concerning how to close the account, notify a financial institution of the fraud, and/or ask credit reporting agencies to correct a credit report to accurately reflect information about the employee. Employers that consider offering identity theft restoration services should investigate the specific services that a service provider will offer. Among other things, an employer may want to ask (1) whether consultants will offer to obtain a power of attorney from the employee so that the consultant can directly liaise with financial institutions and/or the government to fix a fraudulent account, (2) whether consultants are trained to handle the full range of issues that may arise in connection with identity theft, (3) whether employees will be assigned a specific case manager for continuity, or will be required to recall a hotline each time they have questions or require assistance, and (4) whether case managers/consultants receive commissions for directing employees to utilize a specific product or service (*e.g.*, enroll in credit monitoring, obtain a credit report, etc.)

Identity theft insurance. In the event that an employee is unable to close a fraudulently opened account, or is unable to reverse actions taken by an identity thief, they may experience financial loss or need to retain an attorney to protect their interests (or defend the employee against creditors). "Identity theft insurance" refers to an insurance product that is designed to either compensate an employee for such losses, or defend an employee (*i.e.*, provide an attorney) if a creditor attempts to collect funds related to a fraudulently opened account. Often companies that offer identity theft insurance as part of a bundle of identity theft services are not insurance companies themselves and are merely providing an insurance policy that has been negotiated with an underwriter. Employers should request a copy of the actual insurance manuscript that relates to the offering (not merely a summary of benefits) and review the policy to better understand (1) what benefits will be provided to their employee, (2) what deductibles, if any, the employee may have to meet, and (3) what coverage exclusions exist.

Determining which identity theft service to offer in connection with a particular breach can be complicated and depends heavily on the type of breach that occurred. To better help you

understand which services are appropriate the following chart cross-references types of services with the type of data that may have been impacted in a particular breach:[5]



In addition to understanding which services "match" the type of data impacted, employers must also consider the different ways that identity theft service providers charge for their products. Some providers use a "redemption model," by which they charge employers only for the number of employees that redeem an offer of identity theft services. Other providers use a "capitated model," by which they charge employers for the number of employees to whom an offer of identity theft services is made, regardless of whether the employees redeem the offer.

While redemption pricing appeals to many employers because they will not have to pay for unused services, the per employee price using the redemption model can be as much as 50 times greater than the per employee price using a capitated model. More importantly, the redemption model can make it difficult for an employer to budget for a security incident as the

[5] To the extent that a breach involves multiple data fields (e.g., if a breach of a tax preparer led to the loss of tax information and Social Security Number) you should look to the services that match to both fields.

true cost of the service will not be known until the employee enrollment period closes – which may take several months.

> TIP: While some employers err on the side of providing employees with the full range of identity theft services following a breach, receiving services that don't "match" the data breach can confuse many employees and lead them to incorrectly believe that they are at risk for the types of identity theft that the service is designed to mitigate; not the types of identity theft that may flow from the breach itself.

G. Whistleblower Policies

One of the most important factors that shape how well an organization can respond to a data security breach is how fast the organization discovers that a breach occurred and initiates a formal investigation and response. Put differently, it is hard to respond to a breach, or mitigate its impact, if you don't know that it has occurred.

Employees are an indispensable resource for identifying security breaches. In some cases, they may be the *only* individuals that know that an incident occurred. For example, if an employee inadvertently throws away sensitive information that should have been shredded, the organization may never discover that it occurred until, or unless, a bad actor finds the materials.

In other situations, the organization may find out about an incident too late to mitigate the impact. For example, if an employee inadvertently sends a file that contains sensitive information to the wrong email recipient, unless the employee self-reports, the organization may first hear about it from the recipient *after* they open the file and view the information.

Most HR professionals are familiar with the concept of a whistleblower policy – *i.e.*, a policy that is designed to encourage employees to report their own conduct or the conduct of their peers. While many whistleblower policies are focused on traditional employment-related issues (*e.g.*, sexual harassment, racial discrimination, theft, etc.) some employers have adapted their whistleblower policies to encompass data security-related issues to encourage the reporting of security incidents. Employers should consider the following factors when assessing their whistleblower policies:

- ❑ Scope. Does your current whistleblower policy have a narrow scope that would suggest to an employee that it does not apply to data security-related incidents?

- ❑ Ramifications for self-reporting. If your whistleblower policy does not formally extend to data security-related matters, what would your organization do if an employee self-reported a security incident that they were responsible for causing?

- ❑ Ramifications for peer reporting. What would your organization do if an employee reported that a colleague caused a security incident?

- ❑ Culture. How confident is management that employees would voluntarily report a security incident?

> TIP: Consider adding to whistleblower or anti-retaliation policies a provision that states when an employee reports the employee's own conduct that is in violation of company policies or is contrary to company standards or practices, such self-reporting will be weighed as a positive factor in determining the company's response to that conduct.

H. Practicing For a Data Breach

There is no replacement for training and experience when handling a data breach. In order to gain experience without having to wait for a breach to occur, many employers try to anticipate real life situations that might arise and practice how they would respond. There are generally two formats for practicing for a data breach: tabletop exercises and breach simulations. The following provides a high level summary of the differences.

Tabletop Exercises. Although a tabletop exercise may take many different forms, it typically involves an experienced moderator (*e.g.*, an attorney who focuses on data security breaches) who walks senior management through a data breach scenario and facilitates a discussion concerning how management would likely respond. Tabletop exercises can last anywhere from a couple of hours to a full day. Some provide multiple scenarios that are presented as vignettes. Others try to simulate a real life breach by providing multiple injections of factual information concerning a single breach throughout the day that approximates the type of information that a company might learn over the course of several weeks or months. Regardless of the format, the goal in almost all tabletop exercises is to expose management to the types of issues that might arise in a data breach and to help management understand the strategic decision points that they may confront.

Breach Simulations. Breach simulations are designed to test the ability of an organization to respond to a data breach. For example, a breach simulation of ransomware on an employee's computer would test how quickly the information technology department is able to isolate an employee's computer, whether they are able to restore the employee's files from back-ups, and whether they are able to investigate if data loss has occurred. This simulation would also test whether management is prepared to make strategic decisions (*e.g.*, does the organization pay extortionists, or does it not?). It also might test how HR handles questions that come in from employees, and whether

HR is prepared to communicate with employees who may have been impacted by the incident.

TIP: When planning a tabletop exercise or a breach simulation, it is important to make sure that the person, or entity, that is conducting the exercise has knowledge and experience concerning the range of issues that arise in a data breach. Be careful not to select a moderator who may only have a narrow view of how a breach works or the issues that it may create. For example, while a forensic investigator may be able to design a realistic IT-scenario, they may not fully understand the public relations, legal, and business issues that arise during a breach. Similarly, while a public relations consultant is likely to anticipate the PR-impact of a breach, they may lack experience with the legal, business, and contractual impact.

III.
INCIDENT RESPONSE

The best way to investigate a security incident is to follow an incident response plan that was put in place before the incident occurred and that takes into consideration the specific needs and resources of an organization. If you are evaluating an existing response plan, or if you do not have an incident response plan when an incident is identified, the following steps outline best practices that take into account possible legal requirements and obligations. These include recommendations for investigating the incident, coordinating with data owners, communicating to the public or media, communicating with law enforcement, communicating with employees, and communicating with regulators. This section also discusses unique issues that arise in the context of certain types of employment related data breaches.

A. Investigating a Security Incident

1. Include Legal Counsel at the Inception of an Investigation

When a data security incident is first suspected, consider notifying your in-house or outside legal counsel. A primary benefit of involving counsel early in an investigation is to allow counsel to help you decide whether an investigation should be conducted under the cloak of attorney-client privilege.

The attorney-client privilege and the attorney work-product doctrine are judicially recognized evidentiary protections in the United States that are designed to ensure that a client (*i.e.*, your organization) can provide factual information to an attorney for the purpose of obtaining legal advice without the fear that the communication or information will have to be shared with the government or opponents in litigation. In the context of a data security investigation, there is a strong argument that the following types of communications are covered by privilege:

- Advice from your attorney concerning your statutory, regulatory, and contractual obligations in the event of a data breach.
- Your attorney's opinion concerning the likelihood that you will receive a legal challenge in connection with the incident.
- Ways in which you can lower the risk of litigation.
- Information that your attorney requests be collected in order for your attorney to be able to provide legal advice.

With regard to the collection of information, your attorney may recommend that a forensic investigation be led by your legal department or outside counsel as the information obtained in the investigation may be necessary for your attorney to provide your organization

with legal advice. There are steps you can take to ensure the strongest argument that the privilege should protect the analysis and reports of those investigating the incident. For example, employees who participate in an investigation should copy counsel on all internal communications concerning the cause and the scope of the breach or, when speaking to others, clearly indicate that they are collecting information at the behest of counsel. If information needs to be gathered from IT or HR by email, consider putting in the subject line a clear statement that the communication is an "Attorney Client Communication: Information Requested By Counsel." This helps make sure that anyone who reads the email at a later time understands the context in which it was sent, the purpose for which the information was collected, and the fact that the communication may be privileged and exempt from disclosure outside of the organization.

TIP: Third party forensic investigators are often retained through outside law firms – instead of through an organization's IT department – to make clear that their purpose is to help your attorneys understand the factual situation surrounding an incident in order to provide legal advice. The contract with a forensic investigator often forms the foundation of your ability to assert that their analysis of forensic evidence is privileged.

2. Form a Core Team to Respond to a Breach

Investigating a security incident that involves HR data, or the actions of an employee, often requires a team that may include representatives from Information Technology, Information Security, Legal, Risk Management, Operations, Marketing, Communications, and/or Human Resources. Ideally, a team is selected and trained on data breach response prior to the occurrence of an incident. One person should be designated to keep a log or running chronology of the investigation to enable the organization to reconstruct later what information the organization knew at what time. Personnel should take extreme care when documenting an investigation to avoid creating a factually inaccurate record by recording opinions that may be based on preliminary information.

If a representative from HR is included in the incident response team, they typically serve several functions. First, HR is uniquely situated to understand the impact that a data breach may have on employees. This includes predicting the types of questions that employees are likely to ask and predicting the impact that a security incident may have on morale. Second, HR is often best situated to help the incident response team plan how information about a security breach should be communicated to employees. The method of communication often depends on a number of variables ranging from the size of your workforce, the number of employees involved in the incident, and the organization's normal operating procedure for conveying information. Third, if a security incident involves the actions of an employee (malicious, negligent, or inadvertent) HR may be needed to help investigate the employee motives, to take disciplinary

action (if warranted), or to provide ongoing training for the employee (and perhaps others) about good security practices.

> TIP: Consider designating two people from each department that may need to participate in an incident response team – a "primary" contact and a "back-up" contact in case the primary team member is unavailable.

3. Preserving Evidence

The immediate reaction of many organizations when they discover that a system may be infected with a virus or malware is to remove, erase, and rebuild the potentially infected system as quickly as possible in an effort to clean the environment. Doing so without taking proper steps to preserve evidence, however, may make it difficult to reconstruct whether and what information was lost. Without answers to those questions, the organization may not be able to comply with legal obligations or to accurately identify the level of risk that the breach posed to the organization or to its employees. It also may make it difficult to accurately determine the scope of the breach and ensure notification of the breach to affected employees. In addition, without knowing what happened and how it happened, it may be difficult to have a high level of confidence that the same incident will not happen again.

As a result, when dealing with an electronic breach, organizations must often balance the desire to contain the breach and prevent additional information from being lost with the need to preserve evidence and investigate what happened in the first place.

Your organization should consider utilizing the following five steps to preserve the type of evidence that might be needed to fully investigate an incident.

Keep or forensically image computers: If a computer (including a laptop, tablet, or mobile device) is potentially infected with malware, your IT department may be considering reimaging the computer. However, that would be a mistake because reimaging effectively deletes all of the information and programs on the device. While reimaging a computer may render it clean and provide a level of confidence that it can be returned to use, it may also destroy evidence that might help determine whether information has been lost, and, if so, how much and what type of information. Instead, consider creating a forensically sound image of the device before it is reimaged. A forensically sound image uses software to create an exact "copy" of the device that can be analyzed in the future as part of an investigation. Alternatively, consider issuing the employee a new computer and keeping the potentially infected device segregated in case it needs to be examined in the future.

Don't turn your computer off: One of the most common mistakes that companies make when they suspect that a computer may be infected with malware is to turn off the

computer or disconnect it from its power source. Some types of malware exist only in the computer's active memory – *i.e.*, the memory that exists only when the computer is powered on. When the computer is powered off, the information that is in active memory (including the malware) may be deleted. If that occurs, it may be more difficult for an investigator to determine what initially infected the computer and what the malware did while the computer was infected.

Disconnect computers from the network: Instead of turning a computer off, consider disconnecting the computer from your network and/or disconnecting it from the internet. If malware is present on the computer, and the computer has been sending information out of your organization, disconnecting it should (1) prevent the computer from infecting other computers on your network, (2) prevent a bad actor from contacting the computer, and (3) prevent the computer from sending additional information to a bad actor.

Suspend logs and backup tapes from being overwritten. Most organizations have systems in place that record events that happen within the organization's network in "logs." Unfortunately, some logs can be voluminous and most organizations retain their logs for only a limited amount of time, after which the logs are overwritten by more current information. If you identify a security incident, consider taking steps to stop your logs from being overwritten or lost. This may be as simple as having your IT department change the settings on certain devices, such as firewalls, so that the systems no longer overwrite logs. In other cases, it may require finding space for the additional logs by either (1) increasing your organization's storage space, (2) purchasing additional storage space with third parties that host, or store, your logs, or (3) exporting logs that may exist on your network to external media for storage.

Consider enhanced monitoring. While most organizations have systems in place that monitor some of the activities that occur on their network, often the level of monitoring is limited. For example, many organizations monitor the points at which their network communicates with the interest (their "perimeter") with a firewall which should provide them with an indication of which IP addresses are communicating with the computers within their organization. A firewall typically does not tell the organization the substance of what is being communicated. Firewalls also can't track actions that are occurring within an organization's network. If a security incident occurs, consider deploying additional technology that is designed to increase your organization's visibility as to what is happening on your computers. For example, network packet capture systems physically inspect the data leaving a network so that an organization knows *what* has left in addition to where it has gone. Endpoint monitoring applications are designed to monitor the activities of devices within your network and to detect suspicious patterns of communication between and among your own machines.

TIP: If you believe that one of your computers is infected with a virus or malware, do not turn it off. Instead, disconnect the ethernet cable that connects the computer to your network (or turn off WiFi). By isolating a computer, instead of turning it off, you can preserve evidence while ensuring that the computer cannot leak data.

4. Retaining a Third-Party Forensic Investigator

Many competent IT departments lack the expertise, hardware, software, or personnel to preserve evidence in a forensically sound manner or to thoroughly investigate a security incident. In such a situation you need to be able to recognize the deficiency quickly – and before any evidence is lost or inadvertently destroyed – and recommend that the organization utilize external resources to help collect and preserve electronic evidence and investigate the incident.

When a forensic investigator is retained, they are often tasked with determining whether a data breach has occurred and, if so, answering the following questions:

- **Infiltration.** Infiltration refers to deciphering how a bad actor was first able to compromise your organization's systems. Infiltration is important for a couple of reasons. First, if you don't know how an attacker originally got into your systems it may be difficult to ensure that they won't be able to come in again. Second, if an investigator can determine the point of initial infiltration, they should be able to piece together a timeline which may be useful in determining when information could have become exposed and what information may not have been at risk.

- **Persistence.** One of the first things that most bad actors do once they are in your organization's network is take steps to ensure that they will be able to remain in the network and cannot easily be shut out. For example, they may install malware that acts as a "backdoor" that allows them to enter the network at will, or they may steal the username and password of employees so that these can be used to login in the future. These types of activities are collectively referred to as "persistence."

- **Aggregation.** If a bad actor is able to make it into your organization's network and is looking for personal information about your employees or your customers, they may attempt to take small pieces of data from various sources (*e.g.*, each of your employees' workstations) and combine those pieces into a meaningful collection of valuable data before trying to remove the data from your environment. The process of staging data for later removal is sometimes referred to as "aggregation."

- **Exfiltration.** An attacker's main goal is typically to remove, or "exfiltrate," data from your environment. Establishing how an attacker exfiltrated data is important as it can confirm whether your organization has experienced data loss (*i.e.*, had a real "data

breach"). It also gives valuable insight into the indicators that you should be looking for in the future (and in the past) in order to identify other attempts to remove data from your systems.

- **Containment.** Containment describes the process of stopping a bad actor from continuing an attack. If a bad actor is a current employee, containment may be as simple as terminating the employee or removing their ability to access information within your organization. If the bad actor is outside of your organization (*e.g.*, a hacker), containment typically involves using the information that an investigator has developed concerning how the attacker works (*e.g.*, infiltration, persistence, aggregation, and exfiltration) and finding ways to disrupt the attacker's activities. Containment often refers to short-term fixes for stopping an attack. In many instances, bad actors identify weaknesses in an organization's security that require significant investments of time, energy, and resources to completely address. Containment steps are often designed to buy an organization time while longer term solutions are identified. Investigators are often able to provide containment recommendations based upon their understanding of how an attack occurred.

- **Remediation.** Remediation refers to the long-term effort of fixing any systemic problems that may have contributed to a bad actor's ability to breach an organization's security. Remediation steps may be technical (*e.g.*, installing new devices, monitoring solutions, servers, etc.) or procedural (*e.g.*, training employees about new attack vectors, modifying the process by which employees choose passwords, etc.). Investigators are often able to provide remediation recommendations based upon their understanding of how an attack occurred.

> TIP: When selecting a forensic investigator consider a number of factors including their price, reputation, availability to dedicate resources to an investigation, ability to work well with your IT department, and ability to work well with your attorneys.

5. Assigning a Crisis Manager

Incident response teams are usually comprised of personnel from a variety of backgrounds that represent a variety of internal departments. Because the members of a response team rarely have the same reporting structure, confusion about who has authority to convene an investigation, assign projects, or retain needed resources can lead to inefficiencies.

A predesignated crisis manager who reports directly to, and has authority conferred from, senior management often facilitates an efficient response. The crisis manager should work closely with legal counsel to ensure that attorney-client privilege is maintained. You should consider five key items if you are designated as the crisis manager for your organization:

- **Track Investigation**: Depending upon the complexity of a data security incident, the incident response team may initiate several investigative tracks simultaneously. This is particularly true in the early stages of a security incident when an organization may suspect that data has been lost, but might not have identified the who, what, where, and why connected with the loss. When there are multiple lines of investigation that may be taxing various resources within, and outside of, the organization, it is sometimes difficult for the members of the incident response team to stay on top of the status of investigative tracks for which they are not directly involved. In such a situation, it can be extremely beneficial to have the crisis manager track each of the investigative tracks.

- **Assign Responsibility:** Security investigations often rely upon the involvement of various personnel within an organization, but don't squarely fall within the responsibilities of any one employee. As different team members work to complete pieces of an investigation, the overall progress of the track can stall. In narrow investigations, the crisis manager may take responsibility for the investigative track. In broader investigations that involve multiple lines of inquiry, this may prove to be impossible. In such situations, it is helpful for the crisis manager to assign responsibility to one person to oversee a piece of an investigation, to take ownership of clearing any obstacles that develop, and to report the status of the investigative track back to the crisis manager or to the entirety of the incident response team.

- **Evaluate The Effectiveness of the Incident Response Team:** Sometimes the team called for in an incident response plan is the right one to investigate a particular incident. Other times, what made sense in a vacuum, or worked well on paper, may not be an effective combination in practice. Throughout an investigation, a crisis manager should evaluate the effectiveness of the incident response team. If the crisis manager finds that the team is not functioning efficiently or effectively, they should adjust the team's membership as needed.

- **Report to Stakeholders:** There are often many stakeholders who are interested in the outcome of a security investigation (*e.g.*, senior management, insurers, auditors, third party service providers, law enforcement, etc.). The crisis manager should attempt to identify those stakeholders early on and develop a strategy for providing them with an appropriate level of information on a periodic basis. Note that whenever a crisis manager is considering sharing information outside of the organization s/he should consult with their attorney prior to doing so to understand whether the information is privileged, what impact sharing it with third parties might have, and what steps (if any) might be taken to protect the privilege.

- **Request Sufficient Resources:** A crisis manager should consider whether the organization has sufficient internal and external resources to adequately investigate a security incident. Resources (*e.g.*, personnel and technology) can almost always be

supplemented; however, it is difficult to do so instantaneously. As a result, the sooner that a deficit is identified and a plan put into place to supplement resources, the better.

TIP:	Often the main role of the crisis manager is to make sure that an investigation is coordinated and each of the members of the incident response team has what they need in order to proceed with their assigned tasks.

6. Investigating Employees

When a data breach investigation reveals evidence of possible employee misconduct, an organization should consider the following steps when approaching an investigation.

First, the Human Resources department should be included in the incident response team. HR will have knowledge of company policies, procedures, and past practices applicable to conducting employee-facing investigations. Members of the HR department may also have specific skills and experience when interviewing employees. If any employee who is subject to investigation is represented by a union, then a labor relations specialist or labor attorney should be consulted to make sure that the investigation complies with the collective bargaining agreement and applicable labor law.

Second, consider whether an attorney with employment law expertise should be consulted. Legal issues relating to the investigation of employees can include whether employees may be instructed not to discuss the investigation with other employees; whether interviews can be recorded without the permission of the employee; and whether there are any legal issues relating to employee privacy protections, whistleblower protections, or anti-discrimination protections.

Third, the investigation of specific employees should be consistent with company policies, procedures and past practices, and basic "due process" principles of fairness (such as having interviews conducted by a neutral, disinterested investigator, *e.g.*, someone other than the employee's direct manager).

Fourth, if the breach investigation will likely result in disciplining or terminating an employee, the investigation of that employee's conduct should be thorough and complete, and any discipline imposed should be consistent with similar violations. Since the fairness of the investigation, including any perceived disparity in discipline may be challenged in litigation it is important to strive for consistency in both the process of the investigation and the disciplinary action imposed.

7. Responding to Employee Misconduct

Employee involvement in a data breach can range, in terms of culpability, from an "honest mistake" (no wrongful intent and no negligence) to malicious or intentionally wrongful conduct. Furthermore, evidence regarding culpability may change over the course of an investigation. Nevertheless, if at any time during the course of an investigation it appears that an employee's intentional misconduct, negligence, or incompetence has caused a serious data breach, then the company should immediately consider addressing the risk of further occurrences by taking appropriate action, such as suspending the employee, reassigning job responsibilities, increasing supervision or additional training (depending on the company's assessment of the employee's culpability and competence).

At the completion of the investigation, the company should determine what action to take with respect to the employee (*e.g.*, vindication, oral warning, written warning, suspension, termination, etc.) and promptly inform the employee of that action. The company should consider how comparable misconduct has been treated previously, the employee's past performance and any circumstances that may give rise to a claim by the employee that the company's adverse decision is a pretext for unlawful discrimination or retaliation.

If the company concludes, or has a reasonable basis to believe, that an employee has engaged in criminal conduct, then the company should consider whether to inform the police or other government agency with jurisdiction in enforcing the laws that have been violated. The company should take into account the considerations described in Section III.D ("Communicating with Law Enforcement"), and the advice of its attorneys, in making that determination.

8. Responding to Whistleblowers

Employees who report the mistakes or misconduct of other employees may be protected by whistleblower laws, or by whistleblower policies adopted by the company, from retaliation for having made a report. It is important to remind employees who are the subject of an investigation not to retaliate against such whistleblowers.

The situation is more complicated with respect to self-reporting of misconduct because there are conflicting policy goals at stake: the company wants to create incentives for employees to report potential data breaches, but does not want to create disincentives for violating company policies or performing work in a negligent manner. This situation is best addressed on a case-by-case basis, taking into account all of the circumstances of the particular case (the degree of employee culpability, the seriousness of the breach, the likelihood that the company would have learned of the breach without self-reporting, etc.), rather than a general policy.

B. Coordinating with Service Providers

Organizations are relying increasingly on service providers to carry out vital business operations – including HR functions. Your agreements with your service providers may authorize you, or the service provider, to have access to or possess sensitive information owned by the other entity. As discussed below, state data breach notification laws typically place the onus on the owner of data to notify affected persons when sensitive personal information is wrongfully accessed or acquired. For instance, a cloud provider may possess a database that contains your employees' Social Security numbers. While the service provider maintains the data, the data ultimately belongs to your organization. In most states, if the information is breached, the cloud provider does not have a statutory obligation to notify your employees. However, it most likely has a legal obligation to notify you, its client, who in turn has a statutory obligation to notify your employees.

As a result, when responding to a data breach you should analyze whether the affected information was collected directly by your organization or whether the data belongs to a third party. If the data belongs to a third party, you should consult the contract that you have with the data owner and applicable state data breach notification statutes to determine your notification obligations. In many instances, although the data owner technically has the legal obligation to notify affected persons, the data owner will look to the service provider to make the notification or pay for the costs of notification.

> TIP: Service providers within the same industry can differ remarkably on how they handle a data breach, how they communicate, and what types of services they offer following a breach. Prior to a breach occurring, consider sharing with your service providers your expectations concerning how they will handle a data breach or negotiating specific requirements into the service agreement.

C. Communicating with Law Enforcement

Many security incidents involve a crime that has been committed against an organization. For example, when someone attempts to hack into an organization's network to obtain sensitive personal information about the organization's employees, they may be committing criminal trespass, theft, attempted identity theft, computer fraud, wiretapping, or economic espionage, among a host of other statutory violations. The organization should consider reporting a breach to law enforcement. Among other things, law enforcement may provide assistance stopping the criminal behavior, useful information that may help the organization's investigation of the incident, or prosecution of the culprit. It may also help demonstrate to employees that the organization was diligent in investigating the incident and taking steps to protect employees' data.

There is no single federal or state law enforcement agency with jurisdiction over data breaches. In general, however, you should consider contacting the Federal Bureau of Investigation's Cybercrimes unit or the United States Secret Service with regard to a security incident that involves the electronic exfiltration of information. For security incidents that involve paper records or known individuals (*e.g.*, employees or former employees), you might also consider contacting municipal law enforcement in the jurisdiction in which the perpetrator resides or works.

You should discuss with your attorney whether you may lose the protection of the attorney-client privilege if you provide information to law enforcement. Although recent legislation – including the Cyber Security Act of 2015 – is designed to help companies share information with the government without losing privilege protection, counsel should closely examine the limits of those statutes. The applicability of such legislation typically depends upon the type of information shared, how the information will be used, and the law enforcement agency with which it will be shared.

TIP: Consider developing relationships with law enforcement in your area before a breach occurs. Different agencies (and even different officers or agents within the same agency) respond to data breaches in remarkably different ways. The more you know about how your law enforcement resources are likely to respond, the more comfortable you may feel consulting them when an issue arises.

D. Communicating with Impacted Employees

Federal data breach notification statutes apply to financial institutions, health care providers, and vendors of health records. Although dozens of proposals have been made for a federal data breach notification statute that would apply to other types of organizations, as of the publication date of this chapter there is no national data breach notification law that applies to most employers. Instead, 48 states, plus the District of Columbia, Puerto Rico, Guam and the Virgin Islands, have enacted their own statutes addressing an employer's notification obligation in the wake of a data breach involving certain types of personally identifiable information. The only states without such laws are Alabama and South Dakota, although employees that reside in these states may be covered by the data breach laws of other states.

Although state data breach laws are not uniform, the laws are more similar than not. The following summarizes the key provisions of state data breach notification laws and highlights areas in which state laws diverge. In the event of a breach involving records of employees who live in multiple states, the laws of each state should be reviewed to ensure that the organization is complying with all of its notification requirements.

1. Do State Laws Apply to Your Organization?

As a general rule, you should consult the data breach notification law of (1) the state in which your organization is headquartered, and (2) the state (or states) in which the employees who have been impacted by a data breach reside. Some states maintain that "any entity" is subject to their data breach notification law, while other states limit applicability only to those entities that "conduct business in the state." Most of the statutes place the onus on the "owner or licensor" to ensure that affected employees are notified, however, some states (*e.g.*, Rhode Island and Wisconsin) place that obligation on organizations that simply "maintain" employee information. As discussed below, even if the breached organization does not own or license the employee information, most state laws will require that the organization timely notify the data owner of the breach so that they may notify the employee.

The state notification laws typically apply only to employees who are residents of the state in question. However, Hawaii, New Hampshire, and North Carolina's statutes do not contain this limitation and apply instead to "affected persons," while Texas's statute specifically applies to Texas residents and residents of other states. The language of these statutes could be argued to cover notification to residents of Alabama and South Dakota, the two states that have not yet passed their own notification law.

2. What Personally Identifiable Information Triggers Notification?

State data breach notification statutes generally require notification in the event of breaches involving the following information: an employee's name in combination with their Social Security number, driver's license number, account number, and access code. Some states go further and require notification in the event other types of information are accessed or acquired. For example, Iowa, Nebraska, North Carolina, Oregon, and Wisconsin all require notification if biometric data is breached (*e.g.*, an employee's fingerprints). North Dakota requires notification if an employee's date of birth or mother's maiden name are exposed, since that data is often associated with password recovery or identity verification on online accounts. Arkansas, Missouri, Puerto Rico, Montana, Nevada, Oregon, Rhode Island, and Texas require notification if certain types of medical or health information are at issue. Montana and Wyoming recently expanded their definitions to include taxpayer identification numbers.

California amended its statute in January 2014 to become the first state to require employee notification in the event of a breach involving a username or email address in combination with a password or security question and answer that would permit access to an online account. If this type of information is lost, the notification that you provide to an employee should direct them to promptly change their password and security question or answer, as applicable, or to take other steps to protect all online accounts for which the employee uses the login information. Other states, such as Florida, Wyoming, Rhode Island, Nevada, and Illinois have since enacted similar changes to their data breach notification statutes.

The state statutes provide that breach of personal information that is publically available does not give rise to a notification requirement. Similarly, the breach of personal information that is encrypted generally does not give rise to notification obligations, because data is assumed to be sufficiently protected from disclosure if accessed in its encrypted form. At least one state – Tennessee – no longer assumes, however, that encryption always protects information.

Because not every breach of personal information is likely to lead to a risk of harm to an employee, many states have included a materiality threshold that limits notification to only cases where the breach "compromises confidentiality, integrity, or security." A handful of states do not contain any such limitation, however, and appear to require notification in the event of any breach, regardless of whether an employee is actually at risk of harm.

3. How Quickly Must You Notify Affected Employees?

Most of the state statutes do not strictly define the timing in which notification must occur. Only a few states prescribe specific deadlines (*e.g.*, Wisconsin (45 days), and Florida (30 days)). Generally, the notification must occur in the "most expedient time possible and without unreasonable delay." How this language is interpreted may vary but, as a general rule, you should endeavor to notify affected employees within 30-45 days. The triggering point is generally the date on which you determined that a breach exists or the date that you had a reason to believe a breach may have occurred. All states will permit an organization to delay notification if law enforcement determines that notice to individuals would interfere with a criminal investigation. If your organization intends to delay notification based upon a request by law enforcement, consider obtaining written confirmation of that request to explain any delay at a later time.

4. What Information Does the Notice Have to Include?

Many state laws do not provide any instruction or requirements concerning the content of a notification, leaving the content to the discretion of the employer. Other states mandate that some or all of the following information be included in a notification letter: (1) a description of the breach; (2) the approximate date of the breach; (3) the type of personal information obtained; (4) contact information for the credit reporting agencies or for relevant government agencies; (5) advice to the employee to report suspected identity theft to law enforcement and/or a reminder to be vigilant about identity theft; and (6) a toll-free number that employees can call with questions about a breach. However, because there are many deviations from what the states require, each individual statute should be examined in connection with reporting a breach. California, for example, proscribes specific headings that should be included in the notification letter.

Massachusetts's statute contains a significant departure from the other states in that it *prohibits* an organization from identifying the nature of a breach. Thus, in a nationwide breach, you should consider whether Massachusetts employees should receive a slightly modified notification letter compared to the one sent to residents of other states. In addition,

Massachusetts and Illinois both prohibit companies from providing in the notice the number of those states' residents impacted by a breach.

5. How Must an Organization Notify Affected Employees?

The majority of states require that employees be notified in writing. If your organization has a large number of employees, email notice can provide substantial cost savings over mailing written notice, but notification through email is only permitted in approximately one-third of the states and in those states there are restrictions on when email notice is permissible. For example, many states require that an employee either consent to receive electronic notices, or that the primary method of communicating with the employee has been through email, such that the employee would not be surprised to receive email notification. Additional states permit email notification if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001, the federal ESIGN Act.

If your organization is thinking of sending an electronic notice, you should consider the risk that third parties may attempt to create fake electronic messages that appear to originate from your organization (a practice called "spoofing"). These messages can further victimize employees by having them provide additional personal information (a practice called "phishing"). For example, instances have been reported where individuals send fake notification emails that ask employees to click on a link that, in turn, downloads malware onto the employee's computer. In other cases, the fake notification email requests that the employee respond with personally identifiable information to a service allegedly providing credit monitoring. As a result of these risks, some companies have chosen not to send electronic messages concerning a security breach. Or, some companies make clear in the emails that they do send that they will never request that employees transmit additional personally identifiable information over email or click on a link to obtain credit monitoring. In other situations, companies have determined that the risk of phishing is low and have opted (where permitted) to notify employees by email. For example, if you have a relatively small number of employees, the likelihood that a bad actor will attempt to phish your employees based upon a data breach notification may be insignificant.

Most states permit "substitute notification," which is typically some combination of email, posting information about the breach on the organization's website, and/or notifying the media. The circumstances under which such notice is permitted vary widely. Substitute notice generally is permitted only when notification costs are great and/or the number of persons to be notified is large. For example, Arizona permits substitute notification if the notification cost exceeds $50,000, or the number of affected persons exceeds 100,000, or if the organization has insufficient contact information for affected persons. New Jersey (and many other states) will not permit substitute notice unless the cost exceeds $250,000, the class exceeds 500,000, or if the organization has insufficient contact information for affected employees.

Many states permit an organization to create its own notification procedures for the treatment of sensitive personal information if its internal procedures comply with the timing requirements under the state law. If notification is done in accordance with the organization's policy, the organization is considered to have complied with the state law.

6. Should an Organization Ever Voluntarily Notify Employees of a Breach?

Notice is not required by any state or federal laws in most data breaches that don't involve highly sensitive data, such as Social Security numbers. There are many situations in which an organization may choose to voluntarily notify employees, however. For example, although California and Florida currently are some of the growing number of states in which notification is required for a breach of electronic account user names/email addresses and passwords, if such a breach also involved employees in other states, the organization may want to notify all affected persons for consistency.

In addition, breaches often become public through other means (*e.g.*, internet blogs or the media). Self-notifying, even when such notification is not legally required, may help an organization frame the message before the message is framed for it by a third party. Although the organization may face initial criticism for its data security practices, employees may ultimately appreciate an organization's candor in disclosing a breach.

7. Is Notification Required To Any Other Parties?

Various state statutes also require employers to notify third parties. For example, some states require an organization to notify the three major credit reporting agencies in the event of a breach involving a minimum number of employees (typically, at least 1,000). Statutes with such a requirement generally do not set forth what information should be provided to the credit reporting agencies other than the timing, distribution, and content of the notices that the organization intends to send to consumers.

About one-third of the states have a requirement that the state government (usually the Attorney General's office) be notified of a breach under certain circumstances. Of those states, most require notification in the event of a breach involving any number of employees, while others require that the breach impact a minimum number of residents before the notification is necessary. For example, Hawaii, Missouri, and South Carolina only require state government notification if a breach involves at least 1,000 residents.

For states requiring government notification, the statutes again vary on what information is required to be reported. Most states will require that the reporting organization provide a copy of the breach notification letter that was sent to employees, identify the number of residents notified, and provide the timing of the notification. At least Indiana, North Carolina, and New York have prepared online forms for use in connection with government notice of a breach. In

the event of a multi-state breach, each statute should be carefully examined to ensure full compliance.

E Unique Issues Relating to Specific Types of Breaches

There are several common types of data security incidents that frequently impact employers. The following sections explain these common types of data breaches, provide context that may be useful if they impact your organization, and include specific tips to keep in mind if you are faced with such situations.

1. Lost Laptops and USBs

One of the earliest ways in which data was lost – and still one of the most common – is when a mobile device like a laptop, USB thumb drive, or smart phone goes missing. As companies increasingly embrace flexible work schedules and let employees determine when and where they will do their jobs, the data security risk if one of these devices is lost or stolen should be carefully examined. To address these risks, some companies have adopted policies that bar the use of a USB thumb drive or, at a minimum, require that the USB thumb drive be encrypted and password protected.

With respect to laptops, companies should ensure that they are password protected, the passwords are frequently rotated, and, if possible, that access to the company's virtual site be subject to multi-factor authentication (*e.g.*, a physical token with a constantly rotating numerical password or a second login requesting information that only an authorized user would know, etc.).

Some companies have decided to require employees to provide their own portable devices, commonly known as "bring your own device" policies. While such policies can result in significant cost savings for the company, from a security perspective, there are concerns. Companies should ensure that any personal devices used for work-related purposes contain either full-disk encryption or the ability to remote wipe the device.

> TIP: Employees should be trained on good data security practices when connecting to public Wi-Fi networks. Using a virtual private network (VPN), which allows you to access the internet using a private network while on public Wi-Fi, can significantly decrease the risk that your data may be compromised.

2. Errant Emails

One of the easiest ways in which data can be lost – literally in the blink of an eye – is when an email is inadvertently sent to the wrong person. Anyone who has ever done this is

familiar with the immediate sense of panic that follows when you realize that the private email meant for your colleague actually went to your boss. In the data security context, this can be particularly problematic when the errant email contains personally identifiable information which, if sent to the wrong recipient, might pose a threat to the data.

Companies should encourage employees to self-report immediately upon realizing that an email was sent to the wrong person. The recipient usually should be contacted right away and asked to delete and not read the email. Depending on the sensitivity of the information and the recipient, the company may wish to ask them to confirm in writing that the email was deleted, the attachment was not opened, and they did not share the email with anyone else. Legal counsel should be consulted to determine if the data breach statutes would require notification to the affected individuals or whether applicable laws permit the company to do a risk of harm analysis to determine that notification is not necessary. If a risk of harm analysis is permitted, the specific facts involved often drive whether notifying individuals is necessary. For example, if a data file is inadvertently sent by an employee of your organization to client X instead of client Y, but the person that received the file at client X has confirmed, in writing, that they deleted the file before opening it, made no copies of the file, and did not view its contents, there is a strong argument that the confidentiality and integrity of the data file was not compromised. If a state data breach notification statute only requires notification where there is a compromise of the data's confidentiality or integrity, notifying the impacted individuals may not be needed. Conversely if a data file is inadvertently sent by an employee of your organization to a former colleague who had been terminated for misusing company information, and the recipient is not willing to verify that s/he has not opened the file, there may be reason to believe that the confidentiality and integrity of the data file was compromised which, in turn, may trigger some state breach notification statutes.

TIP:	Many errantly sent emails are the result of the "auto-complete" feature available in most email software programs, like Outlook. Although this feature is convenient and efficient, to avoid inadvertently sending an email to the wrong recipient, your company may want to disable auto-complete from company computers.

3. Tossed Files

Many employers know that they should protect sensitive information relating to employees that is in their possession but mistakenly think that the need to protect information ends when they no longer have a use for it. At least 31 states and Puerto Rico have enacted laws requiring data destruction or disposal of personally identifiable information that renders it unreadable, unusable, and undecipherable. Some of these statutes give examples of proper disposal methods of both electronic and paper documents, including shredding, burning, pulverizing, destroying, or erasing information. Some of these states impose a civil penalty per person when a company fails to ensure that personal information is not securely disposed.

Companies should develop and implement a data retention policy that governs how long employee personal information will be kept and sets forth a plan for the destruction of both paper and electronic records containing such information. The policy should ensure accountability by designating a specific person or department to take ownership of ensuring data destruction occurs after an employee leaves the company and the information is no longer required to be maintained. The designated person should be required to certify that such information has been securely destroyed, including identifying all sources of that information. Because simply deleting electronic information may not actually permanently erase it, your IT department should be consulted on methods for ensuring permanent removal of information from company hard drives.

TIP: If you provide information about your employees to a business partner who assists your company with facilitation of employee-related services (*e.g.*, benefits, payroll, etc.), your contract should set forth clear expectations for the destruction of personal information after an employee leaves your company. The person within your company who is in charge of data destruction should also be tasked with communicating with business partners when an employee leaves.

4. Tax/W-2 Breaches

Tax returns and W-2s are information rich documents that contain the name and Social Security number of an employee, as well as information concerning their salary and address, and personal behavior and characteristics (*e.g.*, the charities that they support, their sources of income, their investments, and their relationships with financial institutions). Each year cyber-attackers target these documents to sell sensitive information contained in the file. Other attackers may attempt to use tax documents (*e.g.*, an employee's W-2) to submit a fraudulent income tax return in the hope of defrauding the IRS into sending funds for a false tax refund.

There are many methods by which attackers attempt to obtain tax information, including obtaining tax documents from employers. For example, in 2016, IRS Commissioner John Koskinen highlighted spear phishing attempts against human resource departments: "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

Employers should consider taking the following steps to help prevent a data breach of your employee tax records:

1. If you receive a request from a company executive to email large quantities of employee information, verify that request by telephone before responding.

2. If the request appears legitimate, consider transmitting the data using a secure connection and not by email.

3. If you need to transmit tax information by email, encrypt the document before sending it.

4. Never use a formulaic or easy-to-guess password for an encrypted file (*e.g.* employee's last name).

5. Do not publicly post any information that your employees may need to access their tax information online.

6. Track the rate of tax fraud reported to your Human Resource department each year. If the quantity of tax reported fraud is significantly greater this year than it was in previous years, consider investigating whether data may have been breached.

If you have fallen victim to email phishing, talk to your attorney about whether you are required to notify your employees and whether it makes sense to provide employees with credit monitoring services.

TIP:	Data breaches involving tax information have increased dramatically over the past few years. Most of the attacks involve tricking your employees through social engineering. Training employees to be mindful of attempts to gain employee information around tax season, and drilling home basic security hygiene are the best ways to help prevent this type of data breach.

5. Unauthorized Authentication to Service Provider Accounts

Service providers that permit your employees to establish a user name and/or password in order to log into an online portal often monitor employee accounts for indications that an unauthorized person has obtained an employee's username and/or password and attempted to login. If an unauthorized person does log into an employee's account, it is sometimes referred to as "unauthorized authentication."

Unauthorized authentication does not always mean that a "data breach" has occurred. In most cases what the bad actor was able to see, or download, once they logged into an employee's account determines whether the incident meets the definition of a data breach under the data breach notification statutes. For example, if an attacker obtained an employee's username and

password (*e.g.*, guessed the user name and password, or obtained it from an unrelated breach) and used it to log into an account that contained the employee's salary, or that contained data elements that the attacker already possessed (*e.g.*, the username and password that the attacker used in the first place), the incident would not be considered a data breach.

Depending upon the circumstances, unauthorized authentication may not be a cause for alarm regarding your service provider's security practices. Unauthorized authentication occurs in almost every situation in which users are permitted to access an account online – *i.e.*, eCommerce websites, online email platforms, financial accounts, etc. While there are steps that companies can take to make unauthorized authentication more difficult (*e.g.*, two-factor authentication) no online login system is perfect. Employers should focus on whether their service providers take steps to monitor for unauthorized authentication and report unauthorized authentications when they do happen to the organization.

TIP: "Unauthorized authentication" should not be confused with a data breach. Typically unauthorized authentication does not indicate that an organization's network was compromised, or that sensitive information was lost from the organization. Rather unauthorized authentication is often the identity theft that occurs against your employee as a result of an earlier (and often unrelated) breach where their access credentials may have been originally stolen.

6. Breaches Involving Health Information

Employers that operate a self-insured health insurance program may be subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the event of a breach. Although HIPAA is a federal law, it does not preempt state laws that provide even greater protection of patient information, so state laws may still need to be examined in the event of a breach involving protected health information ("PHI").

PHI is defined as any individually identifiable health information that is transmitted or maintained in any form or medium; is held by a covered entity or its business associate; identifies the individual or offers a reasonable basis for identification; is related or received by a covered entity or any employer; and relates to a past, present or future physical or mental condition, provision of health care or payment for health care to that individual.

Entities that are directly covered under HIPAA include healthcare providers (*e.g.*, doctors or hospitals) that conduct certain transactions in electronic form, health plans (*e.g.*, health insurance companies), and healthcare clearinghouses (*e.g.*, third-party organizations that host, handle, or process medical information). It also includes self-funded health insurance plans. HIPAA also creates obligations for "business associates." A business associate is any person or organization, other than a member of a covered entity's workforce that performs services or

activities for, or on behalf of, a covered entity if such services or activities involve the use or disclosure of PHI. For example, business associates can include third-party claims administrators, billing agents, consultants, attorneys, or accountants who provide services for a covered entity that involves access to PHI, or a medical record transcriptionist. HIPAA requires that the covered entity contractually require the business associate to comply with the privacy and security rules under HIPAA.

The HIPAA Breach Notification Rule requires covered entities to provide notification of a breach involving PHI to affected individuals, the Secretary of the United States Department of Health and Human Services, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate. The timing of the notification to the Secretary depends on the number of persons affected by the breach. If the breach involves 500 or more persons, then the Secretary must be notified without unreasonable delay. For fewer than 500 persons, notification may be made on an annual basis.

Covered entities are also required to have in place written policies and procedures regarding breach notification, to train employees on these policies and procedures, and to develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

TIP:	Many employers think HIPAA only applies to doctors, hospitals, and insurance companies. If you maintain a self-funded insurance plan remember that HIPAA applies to your organization as well.

CONCLUSION

Planning for how your organization will respond to a security breach is essential to being prepared to quickly and efficiently handle a data security breach. As the data security laws are evolving and changing almost as quickly as the threats to an organization's data, HR professionals play a vital role in helping an organization respond quickly and efficiently when a breach occurs.

Bryan Cave LLP

Bryan Cave LLP is a global law firm with more than 900 highly skilled lawyers in 26 offices in North America, Europe and Asia. The firm represents publicly held multinational corporations, large and mid-sized privately held companies, emerging companies, nonprofit and community organizations, government entities, and individuals. With a foundation based on enduring client relationships, deep and diverse legal experience, industry-shaping innovation and a collaborative culture, Bryan Cave's transaction, litigation and regulatory practices serve clients in key business and financial markets.