Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Executing a lockdown on

Cyber-security threats

An e-Book publication sponsored by NAVEX GLOBAL®
The Ethics and Compliance Experts

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

NAVEX GLOBAL®
The Ethics and Compliance Experts

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the FORTUNE 100 and more than 12,500 clients, our solutions are informed by the largest ethics and compliance community in the world. For more information, visit www.navexglobal.com.

Inside this e-Book

Preparing your board for cyber-security oversight

Every board knows its company will fall victim to a cyber-attack and, worse, that the board will need to clean up the mess and superintend the fallout. Columnist **John Stark**, a long-time student of cyber-security risks, breaks down the fundamentals boards must establish for cyber-security, and how you can prepare your board to understand those elements and put them in place.

Cyber-attacks can be extraordinarily complicated, and once identified, demand a host of costly and detailed responses—including digital forensic preservation and investigation, notification of a broad range of third parties and other constituencies, fulfillment of state and federal compliance obligations, potential litigation, engagement with law enforcement, the provision of credit monitoring, crisis management, a communications plan; the list goes on. And besides the more predictable workflow, a company is exposed to other even more intangible costs as well, including temporary or even permanent reputational and brand damage; loss of productivity; extended management drag; and harm on employee morale and overall business performance.

So what is the board's role amid this complex and bet-the-company workflow? Corporate directors clearly have a fiduciary duty to understand and oversee cyber-security, but there is no need for board members (many of whom have limited IT experience) to panic.

David Fontaine, former general counsel of Altegrity, which owns Kroll, a top-tier provider of incident response services, explains the dynamic: "Cyber-security engagement for members of the board does not mean that board members need to have computer science degrees or personally supervise firewall implementation or intrusion detection system rollouts. Instead, board oversight of cyber-security entails, most importantly, asking the right questions and being thoughtful, deliberative and informed about cyber-security and its attendant risks."

Along those lines, below is a list of topics and questions relating to one of the more important cyber-security considerations for corporate directors: cyber-security policies and procedures. It is a good starting point to facilitate meaningful board oversight and supervision of a company's cyber-security risks and vulnerabilities.

Incident Response Plan. Just like a fire evacuation plan for a building, a company should have a plan to respond to data breaches; a plan less about security science and network fortification and more akin to the relatively new nomenclature, so-called "incident response." In the absence of an incident response plan, many organizations allow what could have been a relatively contained incident to become a major corporate catastrophe, because they neither thought through all of the elements necessary for an effective response, nor put the necessary mechanisms in place to ensure these elements were addressed in their plans.

Is there a current incident response plan? If so, when was the plan last updated? Who prepared and approved the plan? What are the general principles of the plan? Has the company ever run any mock exercises to test the plan's efficacy? Does the plan contain a current network topology diagram that is adequately documented and, if so, is it pe-

riodically re-assessed and revised as internal systems and external factors change?

Overall Approach to Cyber-Security. Bret Padres, former agent with the U.S. Air Force Office of Special Investigations, who led incident response for the government, now managing director of incident response at Stroz Friedberg, often encounters companies where cyber-security is not properly prioritized by executive management. "Cyber-security is a business imperative, yet too often we are surprised to encounter situations where cyber-security is too far down on a C-Suite priority list—or because it is so complex, simply delegated to lower-level technical personnel," Padres explains.

Is there a commitment from the top down, both culturally and financially, to rigorous cyber-security? Who in leadership is driving the agenda? Is it a C-level accountability and part of the day-to-day business focus? Do current reporting lines and assigned areas of responsibility make sense? Given the responsibilities and accountability needed to execute the incident response plan, are the right employees, possessing the appropriate skill sets, adequately empowered? Is the individual charged with overseeing cyber-defense the same person who reports up the chain about breaches and who would oversee any response–if so, does that dual-rule indicate a conflict of interest?

Business Continuity Plans in Case of Cyber-attack. The importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet too often such plans are not evaluated in the context of assessing cyber-security risks.

Has the company properly evaluated the effectiveness of its business continuity plan in the context of a cyber-attack? Does the business continuity plan need to be reconsidered and refreshed with these additional considerations in mind?

Personnel Continuity. Competition for talent in the information security space is intense, while the pressure on IT security senior executives is infinite and exhausting. Moreover, despite their rapidly rising salaries, turnover remains constant and there is a serious shortage of experienced and capable IT senior executives. What is the company doing to recruit and retain IT security talent?

Relatedly, when a company loses key senior IT security personnel, it is not only a red flag but also an opportunity for a board to examine succession plans, and to obtain an unbiased, albeit possibly disgruntled, view of any cyber-security flaws. The art and the benefit of the exit interview is lost on so many companies today–too often because departing employees are dismissed as resentful and unreliable. In the case of a resigning IT executive, a proper exit interview may reveal critical cyber-security weaknesses.

Keeping Up With Cyber-Security Threats. Staying current about the latest cyber-security

"Preparedness is key, and keeping up with the latest developments in cyber-security and the latest tools and techniques being utilized by cyber-attackers is a career within itself—which requires relying on subject matter experts, including those who build relationships with law enforcement."

Nick Oldham, Former Counsel, Cyber-Security Investigations, Justice Department

trends, software patches, data breach techniques, and so forth requires continual educational efforts and outreach. Like meeting with the neighborhood beat-cop to stay informed about local crime, staying current on cyber-security threats similarly requires liaison efforts with federal and state law enforcement and regulatory authorities. Nick Oldham, former counsel for cyber-investigations at the Justice Department's National Security Division, now counsel at King & Spalding, says preparedness "is key and keeping up with the latest developments in cyber-security and the latest tools and techniques being utilized by cyber-attackers is a career within itself—which requires relying on subject matter experts, including those who build relationships with law enforcement."

What steps does the company take to liaison with law enforcement and regulators regarding emerging cyber-security modus operandi? How has the company considered the rules, practices, and procedures governing the sharing of intelligence with government agencies? Is sharing customer information with federal and state law enforcement authorities permissible or even tolerable, given the sensitivities customers may have toward the privacy of their data?

IT Budgeting. Cyber-security budgetary priorities can shift quickly, and a yearly budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats.

How does cyber-security budgeting work? How are emergency items identified and funded? Does the budget appropriately provide for contingencies in the event of a cyber-attack or cyber-security need?

Training Programs. The weakest link of cyber-security vulnerability at any company will always be its employees, so proper cyber-security employee training is critical.

How often and how effective are the firms' cyber-safety training programs? Who participates in the training, and how does the company handle policy violations, especially violations by senior executives, who studies have shown are typically the least compliant with cyber-security policies?

"Cyber-security engagement for members of the board does not mean that board members need to have computer science degrees."

David Fontaine, former General Counsel, Altegrity

Unfortunately, the public's view of cyber-attack victims is less about understanding and sympathy, and more about anger and vilification. Given in particular the 47 or so separate state privacy regimes, together with a growing range of federal agency jurisdiction, instead of accepting a helping hand, cyber-attack victims are accepting service of process of multiple subpoenas. Rather than being treated like criminal victims, companies experiencing data breaches are often treated like the criminals, becoming defendants in federal and state enforcement actions, class actions, and other proceedings.

To make matters worse, this is just the beginning of a new era of data breach and incident response, where trying to avert a cyber-attack is like trying to prevent a kindergartener from catching a cold during the school year. Members of corporate boards therefore have no choice but to become actively involved in ensuring the organizations they oversee are adequately addressing cyber-security, approaching the subject much the same way an audit committee probes a company's financial statements and reports: with vigorous, skeptical, intelligent, and methodical inquiry. ■

John Reed Stark is President of John Reed Stark Consulting (www.johnreedstark.com), a firm that advises companies and their boards on cyber-security.

Mitigating cyber-threats from the inside out

While companies have become more skilled over the years at defending against outside cyber-attacks, it's the insider threats that are still throwing them for a loop. **Jaclyn Jaeger** explores what types of inside attacks are plaguing companies and what steps they can take to arm themselves.

As attacks on corporate networks become more common, companies are getting more adept at protecting their most valuable assets against cyber-threats outside the company. But it's the insider threats that continue to elude many.

Not all insider threats are malicious or intentional, so it is paramount that companies differentiate between the two. An internal employee who unknowingly grants unauthorized access to a user who has malicious intent—as opposed to an employee with access to sensitive corporate information trying to snitch it from the company—demand different response tactics.

"One common misconception about building an insider-threat program is that it's implying distrust of everyone in the organization," says Randy Trzeciak, senior member of the technical staff for the Software Engineering Institute's CERT Program. "There is a clear difference between insiders who are granted authorized access to certain assets and the threats they could pose to those critical assets."

Another common misconception among companies is that insider threats can be mitigated merely by implementing tools or technology that can identify anomalous activity or behavior. "That's a static solution to a dynamic problem," says Keith Lowry, senior vice president of business threat intelligence and analysis at Nuix, an information management technology firm. "The first thing they have to do is recognize that this is a risk management problem, not merely an IT problem."

One of the most important measures toward establishing a robust insider threat program is to have clear practices and policies from the beginning, supported by advocacy from the C-suite. Those practices and policies should describe, for example, what the program is, the scope of the program, who is responsible for the program, and how to communicate the program.

Policies and procedures are irrelevant, however, if individuals are unfamiliar with them, so improving processes and awareness through training and education is also essential. Companies may want to consider chanting the same "if you see something, say something" mantra that the Transportation Security Administration uses in airports, Trzeciak says.

Another major source of headaches: Employees who continue to be fooled into giving valuable corporate insider information to malicious actors through phishing scams or by being tricked into replying to e-mails that look like they are from legitimate sources, but really are not. This is a persistent security issue, and the companies that will be the most effective in addressing it will be those that give straightforward, simple instruction, says Ari Kaplan, principal of Ari Kaplan Advisors, a legal analyst firm.

A basic prevention, for example, would be to instruct staff members not to open any e-mail that looks unfamiliar or suspect and to forward it instead to their IT team. However, actually getting people to act on that can be easier said than done,

so testing can help test whether or not the education is working. Kaplan says, the IT department will conduct simulated threats posing as a phishing scammer to see what actions employees will take.

According to a report Kaplan authored, 39 percent of 28 information security officers interviewed cited "fear" as the most effective messaging strategy when educating employees about insider-threats. As one security officer at a life-sciences company put it, "best practices work best at higher levels of the organization, but fear is more effective with lower-level staff."

The overall consensus was that mandatory training, praise for positive actions, and relevant examples from personal and professional perspectives are the most effective techniques for overcoming inadvertent employee errors, according to the report.

Furthermore, if an employee or supervisor identifies anomalous activity or behavior, they should have the ability to confidentially or anonymously report the issue to an appropriate stakeholder—ideally, a senior-level executive with the authority to investigate the potential insider threat. Such suspicious activity may involve an employee who is downloading information at a higher volume than other employees, for example.

Security experts further recommend that various departments—such as IT, HR, security, legal, and compliance—be involved in the insider-threat program, which makes for a much more powerful layer of defense. "You're starting to see a much deeper integration between those groups," Kaplan says. "That integration is increasing the level of protection at a lot of organizations."

Tracking threats

Another important measure toward mitigating insider threats is to identify what data merits protection, and from whom. Who has authorized access to those critical assets? In what ways could individuals compromise those assets? "Different threats to different assets require different protection and detection strategies," says Trzeciak.

Tracking insider activity seems to pose the most difficulty for companies. According to the report, most respondents said they are able to identify their critical value data and were capable of detecting who retrieved that data. Those numbers fell to 69 percent, however, when asked about whether their companies know what people did with that data once they had access.

> "One common misconception about building an insider-threat program is that it's implying distrust of everyone in the organization."
>
> Randy Trzeciak, Senior Member, Technical Staff, CERT Program, Software Engineering

One solution may be to allocate roles to users of particular data so that the company can monitor who is accessing it at any time, as one financial services vice president suggested in the report.

Cloud usage and BYOD (bring your own device) policies further increase the risk of insider threats by blurring the line between personal and professional use, and by introducing devices into the workplace that effectively sidestep all official security procedures. For example, if an employee takes a picture of data on their personal smartphone, the employer has no way of knowing. "That's a big challenge organizations are facing, that because it's so much easier now to capture an image of a document on a screen that doesn't necessarily connect back to any sort of monitoring system," says Kaplan.

"If I'm accessing information in the cloud, I have to be mindful of where I'm accessing it and how those protections change depending on where I access information," adds Kaplan. Those are some of the issues that are influencing the way in which companies are evaluating the actions they are taking today, he says.

Testing insider threats

In terms of testing their incident response programs to ensure compliance with current policies and practices, 18 percent of respondents to the report said they conduct annual audits to audit against the policy. In general, most respondents said their companies are testing on a more frequent basis; 68 percent reported engagement in this process multiple times per year, 21 percent tested twice annually, and 32 percent did so at least quarterly.

Certain high-risk events can make a company particularly vulnerable to an insider threat and deserve careful monitoring. For example, based on actual cases CERT has analyzed, employees in a majority of cases stole intellectual property from the company within 30 days of giving their notice, says Trzeciak.

As for as responding to threats, nearly all respondents (96 percent) said they had an incident response readiness policy. Furthermore, the majority (85 percent) said their incident response team included legal counsel, public relations leaders, and crisis managers, among others in finance and accounting, information technology, compliance, regulatory affairs, risk management, law enforcement, privacy, cyber-insurance, and physical security.

If an organization does detect certain activities, at what point do you escalate the issue to an investigation or involve law enforcement? At what point do you take legal action? Companies should be prepared to have answers to those questions, says Trzeciak.

Many respondents said that managing internal threats has received greater investment in the past year. According to the report, 21 percent attributed some of their security team's spending increases to additional protections against internal hazards, and 14 percent of survey participants reported allotting 40 percent or more of their budget to insider threats.

However companies seek to protect themselves, Lowry says he expects that shifting of resources to occur even more in 2016, now that the issue of information security has taken center stage within most companies, and is now as important as profitability and overall good corporate governance. ■

DEFINE INSIDER THREAT

Below, from the Nuix Defending Data Survey, respondents provided their best definition of "insider threat."

When asked to define the term "insider threat," there was a clear theme among the responses, featuring the words "malicious," "internal," "authorized," and "inappropriate."

One financial institution CISO noted: "All threats are insider threats; once a hacker enters the company's environment, it becomes an insider threat."
"Not all insider threats are mischievous," countered another financial institution CISO.

Those nuances characterized many of the other explanations, which varied to include the following simple and complex descriptions:

- A malicious actor who is an internal employee.
- People with access to data trying to sneak it out the door.
- An internal employee who knowingly or unknowingly grants unauthorized access to someone.
- An outside entity trying to get in by taking advantage through social engineering or a relationship to access internal data.
- Any user activity that falls outside of the organization's policy.
- A person who is affiliated with the organization and through negligence or malice puts the organization at risk.
- The usage of inside systems by authorized and unauthorized individuals in a seemingly nefarious way.
- Someone with knowledge of the system who uses that knowledge to create or exploit a weakness.

Source: Nuix

Creating a Culture of Cyber-Security

Five Training Program Imperatives to Address Your Biggest Cyber-Security Risk: Employee Behavior

By Andrew Foose, VP, Advisory Services Team, NAVEX Global

Cyber-security threats are multiplying daily. Needless to say, organizations operating in today's landscape have their work cut out for them.

In the fight against cyber-risks, it's no longer enough to deploy a PowerPoint "training" created by your IT department with basic reminders about passwords and safe-sender lists and expect that it will be effective.

Today's ethics and compliance officers must take a much broader view of what it means to create a cyber-resilient organization. Among those advocating such an approach is Governor Tom Ridge, the first Homeland Security Secretary of the United States and now the chairman of Ridge Global, a team of globally recognized experts who offer clients strategic counsel on identifying, preparing for and mitigating cyber-risk.

In a keynote presentation at NAVEX Global's annual Virtual Conference, Governor Ridge noted, "A cyber-resilient enterprise is more sustainable, profitable, and successful than one that is unprepared to weather a cyber-attack. Cyber-security principles must be embedded into the business at every level: from the board of directors and the C-suite down to line employees, each individual must contribute to a culture of security."

Cyber-resilience requires not only changing employee behavior, but establishing a culture of cyber-security. And who better than ethics and compliance professionals to implement programs that can change culture and impact employee behavior?

High-Quality Cyber-Security Training Is Critical

We often counsel organizations not to skimp on compliance training that addresses their organization's biggest risks—such as workplace harassment and code of conduct. Cyber-security is increasingly critical as studies continue to show that employee training is the number-one way to significantly reduce cyber-security risks. (For a toolkit that provides additional training resources—including sample acceptable use and information security policies, awareness posters, access to a free microlearning course, and more, visit www.navexglobal.com/cybersecuritykit.)

So what are the essentials of a high-quality cyber-security compliance training program?

(1) Emphasize the role employees play in keeping the organization safe.

Teach employees how to identify and report issues using internal reporting channels. The training should cover, at a minimum:

- Who can present a cyber-risk to your organization
- The persistent threat of malware, including on flash drives
- Dangers associated with social media
- Password essentials and how to create strong passwords
- Prevention steps that employees should take
- The importance of immediate internal reporting

» Risks related to mobile devices, public Wi-Fi and unsecure networks

(2) Make sure your training and awareness materials cover the key points in your "bring your own device" and "acceptable use" policies.

> "The human side is where E&C officers can make the biggest impact. This is a chance for the E&C community to step up. Take it."
>
> Governor Tom Ridge

If you don't have these policies in place already, be sure to put them in place. (We offer a free "Acceptable Use" sample template policy on our website to get you started.) Routinely educate your employees on the policy and related updates. (If each employee in a 5,000-employee organization has at least two smart devices, that equates to 10,000+ potential entryways for hackers to access a company's network.)

(3) Include cyber-security in your code of conduct.

Cyber-security is every employee's responsibility, so it belongs in your code of conduct. The NAVEX Global code of conduct, "Doing the Right Things Right" (available on our website) includes a section titled "Protection of Systems & Resources" that reminds employees about the need to keep computer equipment safe and secure and protect passwords, and the business-critical need to protect our data and digital assets.

(4) Incorporate actual data from your organization's security protocols.

Share, for example, the number of intrusion attempts that have been made against your network and how they were identified and stopped. Real-life case studies have a lasting impact on most learners.

(5) Don't forget to train your board of directors and executive team members.

These audiences are just as important as your employee population. Be sure to tailor the content to fit this audience, as it is extremely important they understand the risks involved in managing this growing threat.

Is Your Cyber-Security Training Program Effective?

One way to determine whether your cyber-security compliance training is working is to partner with your IT team to deploy some fake "phishing" e-mails.

Employees who "take the bait" might be required to receive additional training (a micro learning or "burst" short online training course or an in-person refresher). You can also learn something from those employees: Ask them why they clicked, and you may get insights you can use as examples in your next training or your compliance newsletter. For a sample "phishing" e-mail you can use in your own organization, visit www.navexglobal.com/cybersecuritykit.

Ethics & Compliance Officers Have a Unique Role in Protecting Organizations

To quote Governor Tom Ridge addressing compliance professionals:

"Ethics and compliance professionals have the power to accelerate the shift to a culture of cyber-resiliency in their organizations, and better protect their businesses from financial, reputational, and legal risk. The right processes and technologies need to be in place, but the human side is where E&C officers can make the biggest impact. This is a chance for the E&C community to step up. Take it."

Access a Free Cyber-Security Toolkit for Ethics & Compliance Officers

To help ethics and compliance officers establish a culture of cyber-security, we've created a toolkit with a free micro-learning training course, sample acceptable use and information security policies, a sample phishing e-mail, and more. Get your free toolkit by visiting www.navexglobal.com/cybersecuritykit.

NAVEX GLOBAL®
The Ethics and Compliance Experts

ARE YOUR EMPLOYEES CONTRIBUTING TO A CULTURE OF CYBER-SECURITY?

How confident are you that your employees' day-to-day business decisions will result in a strong culture of cyber-security? Different employee groups have unique roles to play. Here are some questions to ask yourself as you consider where you may have gaps and opportunities for training:

Board Members:

» Will they help ensure that cyber-security is built into an organization's governance?
» Do they know what to ask when the IT security team comes into the board room to update them?
» Will they ask the tough questions, or just assume that everything is fine?

Mid-Level Management:

» Will they enforce policies and set the right tone for their teams?
» What will be acceptable and what won't for those they manage?
» Will they look the other way when, for example, an employee brings their unsecured device to the office, or will they be able to explain why that is not okay?
» What steps should mid-level managers take with third-party partners, vendors, and contractors to protect systems on which these relationships and the business depend?

Front-Line Employees:

» Do they understand how their personal responsibility for cyber-security and their online behavior impacts the stability of their company?
» Do they know how to recognize cyber-risks?
» Will they ask the right questions before they act?
» Have they been trained to reduce cyber-risk and report something suspicious?

ANDREW FOOSE

Andrew Foose, J.D., vice president of NAVEX Global's Advisory Services team, is a former senior trial attorney in the U.S. Department of Justice's Civil Rights Division. Andy is recognized among the country's leading experts on conducting lawful and effective internal investigations and has trained thousands of attorneys, compliance officers, auditors and human resource professionals on best-practice investigative techniques and on how to write effective, comprehensive investigative reports. He currently works with organizations ranging from large multi-national companies to smaller non-profits to assess their ethics and compliance programs and to provide guidance on ways to enhance program effectiveness and efficiency.

ABOUT NAVEX GLOBAL'S CYBER-SECURITY TRAINING

Our cyber security compliance training courses were built in close collaboration with industry-leading cyber security experts at Ridge Global. Utilizing the award winning NAVEX Global online training course architecture and design, our courses feature compelling interactive video scenarios based on real-life situations your employees and managers see every day. For a course demo, contact us at info@navexglobal.com or call +1 (866) 297 0224.

ABOUT NAVEX GLOBAL, INC.

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the FORTUNE 100 and more than 12,500 clients, our solutions are informed by the largest ethics and compliance community in the world. For more information, visit www.navexglobal.com.

Smarter Assessments of Cyber-Risk

Every compliance and audit executive wants to manage cyber-security risks. That assumes, however, that the whole organization agrees on what a cyber-security risk *is*. **Jaclyn Jaeger** looks at existing taxonimies to manage cyber-security.

Sure, every compliance and audit executive wants to manage cyber-security risks. That assumes, however, that everybody in your organization agrees on what a cyber-security risk is and how much it threatens you in the first place.

That lack of a basic cyber-risk vocabulary can be one of the biggest impediments to identifying cyber-threats—particularly for multinational companies, with their many different systems and processes. Everyone might agree on the types of data worth protecting, but they may not grasp every point of failure, and every type of failure, that might strike across the enterprise. The cyber-risk assessment, then, would fail.

Enter the cyber-security risk taxonomy.

"The taxonomy is a common language for talking about these risks," says James Cebula, a former technical manager at the Software Engineering Institute (SEI). Cebula co-authored a taxonomy of operational cyber-risks that groups the threat into four broad categories: actions of people; systems and technology failures; failed internal processes; and external events.

For compliance and audit professionals, the SEI's taxonomy can at least provides a way to jumpstart the conversation on cyber-risk. Below is a look at each category, as well as potential points of failure that can arise under each one.

People Risk

Surprising exactly no one, human behavior is the root of most cyber-risk. "The people aspect is a huge area of vulnerability across the board," says Emily Mossburg, a principal at Deloitte's cyber-risk services practice. The SEI taxonomy subdivides this category into risks such as deliberate or inadvertent actions, or not acting at all and failing to prevent a risk. That last category, inaction, typically occurs because of a lack of appropriate skills, knowledge, training, or guidance.

"Everyone needs to understand how security relates to the business and how the business can be impacted by various types of security risks that are out there," says Greg Michaels, an associate managing director with Kroll's Cyber Investigations Practice.

System Failures

"System failures" are the risk that technology doesn't perform as expected, whether that technology is hardware, software, or some integration of the two. A system failure is "generally the first thing that pops into people's minds when talking about cyber-security risks," Cebula says. Most members of the Data Breach Hall of Shame—Target, Home Depot, Neiman Marcus, Michaels Stores, and so on—fall into this category.

"In a number of those cases, a contributing factor had to do with the complexity of the systems, not having a complete understanding of how all the numerous components fit together," Cebula says.

Cyber-risks posed by software failures—a subclass of systems failures—also create vulnerabilities. They can range from improperly configuring software to weak change management that lets the wrong people update software or change settings to improper security settings that might be too lax or too strict.

The increasing integration and complexity of systems also poses a growing risk. "As systems grow larger and more inter-connected, this is becoming a larger area of concern in cyber-security risk," Cebula says.

Companies increasingly use third parties or cloud providers, for example, to handle certain functions; the integration of the third party's systems into your own is often overlooked.

Take Target as a real-world example. Data thieves executed their huge attack against the retailer by gaining access through an HVAC contractor who billed Target electronically. That let the hackers infiltrate Target's financial department, and from there they reached the point-of-sale card readers at cash registers.

"Often times with security incidents that we investigate, or breaches that we help client organizations with, we see that if the third party has a breach, it affects the client organization as well," Michaels says. Doing basic due diligence on third parties that store information on behalf of the company, or that have access to its systems, is important, he says.

That first requires having a firm grasp on what information the company is outsourcing, and to whom it's outsourcing its information, "and making sure that third party has appropriate controls in place is critically important," Mossburg says.

Failed Internal Processes

Failed internal processes happen in the design or execution of those processes. You might have insufficient definition or understanding of stakeholder roles and responsibilities; or inadequate methods to alert you to a potential problem, or to escalate that problem to the right people. Then there is "dropping the ball" risk of inefficiently handing off a task from one person to another.

All those risks demand well-crafted procedures to reduce the chance of mistake. Ask: When something happens, what are the appropriate steps to take? Is the incident response team skilled and conversant in the right procedures? Are the proper procedures in place to deter an incident? Is that team equipped and prepared to respond? "Those all have to do with process design and execution," Cebula says.

External Events

External events are, generally, the easiest to understand. The most visible example is the case of Sony, attacked by North Korean agents to protest the movie studio's distribution of "The Interview." Other examples are data thieves stealing valuable information for resale, or holding your data hostage in a ransomware attack.

The broader lesson that Sony's situation spotlights: that external cyber-risks are unique to each company. (For example, no other company is likely to face a Sony-style attack unless it too releases a film that tweaks the country's dictatorial leader, Kim Jong-Un.)

One point to consider, Mossburg says, is, "Who may be interested in gathering intelligence about your organization? Do you have in place the people, processes, and technology to protect against those threats?"

Prioritizing Risks

Using a cyber-security taxonomy to diagnose your risks is a good starting point. Then what follows is the harder task of ranking those risks in the proper order. Your most valuable data might vary by industry sector (in defense, it might be those plans for a new guidance system; in healthcare or finance, its customers' personal data); systems and processes used to manage that data will vary company by company.

Once your risks are in a rough priority, that allows a more productive discussion with senior leadership on the need to invest in internal controls or monitoring and detection tools. The conversation starts to sound more like a request to invest in specific functions, to support specific business processes and data that deliver X amount of data to the company—a much more productive dialogue with the board or the CEO than pleas for more cash to help fight data breaches.

"It's important for organizations to find an approach that's manageable to them," Michaels says. If you try to take an all-encompassing assessment of cyber-risks, "it's going to be very difficult to manage," he says. A workable roadmap, in contrast, helps a company to start making changes that help minimize cyber-risk. ■

How to simplify cyber-security controls amid abundant laws

Every CCO has heard the warning that it's a matter of when you suffer a cyber-security breach, not if. Then comes compliance with breach disclosure rules—and those demands are becoming as perplexing as the cyber-threat itself. Overwhelmed, compliance officers are seeking ways to navigate these demands and, if possible, consolidate and simplify the training, policies, and internal controls they affect. **Joe Mont** has more.

By now every compliance officer has already heard the warning that it's a matter of when you suffer a cyber-security breach, not if. Then comes compliance with breach disclosure rules—and those demands are becoming as perplexing as the cyber-threat itself.

Virtually every state in the United States has its own breach notification law, and seven of the states have their own laws and regulations for data security standards. A host of federal agencies have their own regulations protecting consumers' financial data, health records, data collection, and more; each with its own disclosure requirements. Then there are the frameworks, such as those from the Committee of Sponsoring Organizations and the National Institute of Standards and Technology, that offer guidance on how to build strong security controls.

Hence companies constantly try to consolidate and simplify training, policies, and internal controls. The task is not easy.

"Businesses that must comply with multiple regulations often find themselves overwhelmed," says Silka Gonzalez, CEO of the Florida-based consulting firm Enterprise Risk Management.

She gives large universities as an example. Because they have medical clinics, they are covered by the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health (HITECH) Act. Providing student loans means compliance with the Gramm-Leach-Bliley Act. Government research triggers the Federal Information Security Management Act. Credit card processing brings Payment Card Industry Data Security Standard (PCI DSS) compliance. All have their own requirements for data protection and post-breach recovery.

To navigate multiple privacy and cyber-security compliance obligations, Gonzalez suggests seeking out commonalities. "When you start reading the requirements of many of these regulations, they are often very similar. Some of the standards, like PCI DSS or ISO 27001, are looking for very similar types of controls and measures," she says.

One practical first step is to create a matrix of all compliance obligations and what they specifically require, to see where they overlap. "When you know the things that are common, you can test

MANY STATES, MANY RULES

The following is a sampling of the variety of state privacy, data, and breach notification laws.

CALIFORNIA: Requires the operators of websites and online services to disclose in its privacy policy how it responds to "do not track" requests and whether third parties are conducting tracking; Websites and online services must post a conspicuous privacy policy; Anyone who notifies more than 500 California residents as a result of a single breach must electronically submit a single sample copy of the notification letter to the Attorney General.

CONNECTICUT: Requires any party that collects Social Security numbers to create a privacy protection policy, posted online, that outlines steps to protect the confidentiality of that information, prohibit unlawful disclosure, and limit access; Breach notification is triggered upon unauthorized access to, or acquisition of, electronic files, media, databases, or computerized data containing personal information when the data has not been encrypted.

MINNESOTA: Prohibits the disclosure of personally identifying information and browsing history by internet service providers without consent.

UTAH: Requires non-financial businesses to disclose to customers, in writing, the types of personal information the business shares with or sells to a third party.

NEW JERSEY: Breach notification is required upon the discovery of unauthorized access to electronic files, media or data containing personal information that was not encrypted.

ALASKA: If an entity determines after an investigation that the breach does not create a reasonable likelihood of harm to consumers, it must document this determination and provide notice of the determination to the Attorney General. The state also maintains an encryption safe harbor in its breach notification law.

Source: Baker & Hostetler

them once instead of 10 times," Gonzalez says. "It's easier to do a comprehensive review of all the areas where they overlap, find major problems, create an action plan, and go and fix them."

Those organizations that are in sectors with heavy government regulation may need to prioritize federal standards and guidance. "Look first to what your primary regulator requires you to do," says Scott Vernick, head of the data protection and privacy practice at law firm Fox Rothschild. "First and foremost, you are going to adhere to the prescriptions and dictates of a primary federal regulator like the Office of Civil Rights if you are talking about protected healthcare information, or the Federal Energy Regulatory Commission if you are a utility."

> "Look first to what your primary regulator requires you to do."
>
> Scott Vernick, Head of the Data Protection and Privacy Practice, Fox Rothschild

Just because a federal agency is on the beat, however, that doesn't mean individual states can be ignored. "Look at the states that are the most aggressive when it comes to these issues, both in terms of what their statutes say and what their reporting and breach notification requirements are," Vernick says. "That doesn't get you out of complying with technical requirements that are applicable to other states, but it will help in terms of planning."

Among the states with the most challenging privacy and data breach notification laws are Massachusetts, California, New York, and Minnesota. Florida even requires the submission of a written incident response plan, Vernick notes.

IT Meets ERM

The growing focus on privacy and cyber-security, and the inherent complexity of having multiple regulatory regimes, is prompting companies

"You don't need to reinvent reporting mechanisms, or even dashboards, for cyber-security. You simply need to leverage them. Rather than reinventing training, it can be bolted onto what is already in place."

Johnny Lee, Managing Director, Grant Thornton

to rethink their approach, moving away from IT ownership and toward integration with risk management efforts. It all reminds Johnny Lee, a managing director at Grant Thornton, of the angst that followed implementations of the Sarbanes-Oxley Act.

"There are cyber-security analogues to any other major category of risk that has registered on the enterprise risk management radar over the last 30 years," he says. With Sarbanes-Oxley, "there was a lot of noise, but ultimately it shook out." Companies eased into the rhythm of using the right frameworks and committing to the needed level of reporting and internal scrutiny. It might not have been easy, Lee says, but it was far from the envisioned nightmare.

Despite the myriad state and federal laws, and competing frameworks addressing cyber-security and privacy, Lee expects history to repeat as companies develop sustainable protocols and view cyber-security as an additional category of risk from an ERM perspective.

"It is imperative to have an enterprise-wide response," he says. "You don't need to reinvent reporting mechanisms, or even dashboards, for cyber-security. You simply need to leverage them. Rather than reinventing training, it can be bolted onto what is already in place."

In looking for a more manageable risk management process, some companies are cherry picking from the various frameworks available. "All have useful roles and relative strengths, but businesses often see both over-engineering and under-representation in them," Lee says. "What they are trying to do, as they did with SOX, is pick a mandatory minimum set of controls and focus all of their efforts on them because they speak most directly to their greatest risks."

Once companies choose the relevant frameworks and standards that best apply to their organization, they will need to map out and classify data, conduct vulnerability assessments, develop an incident response plan, and get a handle on vendor populations and the risks that are associated with those relationships. "You need to understand your compliance obligations, the specific triggering obligations you have, and create a tailored risk profile and strategy," according to Grant Thornton's Lee.

Cyber-security issues may be unique, but they still can fit within traditional risk strategies, says Yo Delmar, a vice president at software vendor MetricStream. To simplify and align the risk management process, making it more manageable, a company needs a common risk and control framework, she says.

Recent guidance from federal regulators, especially those overseeing financial institutions, is pushing front-line units to take on more responsibility for risk assessments. "You will see less of the second line units giving advice and advisory support to the front line, and more risk management functions moving out of it and into the front line," Delmar says. For a company to keep up with this and rationalize all potential conflicts across different regulations, it will need to map those conflicts to the sections of policy and control regulations and best practices of the frameworks that are in scope.

It's a matter of curating that content and mapping it to common controls, risks, and policy sections, Delmar explains, adding that a regulatory change management system is needed to be aware when you might need to rewrite a section of policy, tighten controls, or conduct a risk assessment on a completely new business area. ■

Workflows you need to use post-data breach

Not understanding the steps to take after a data breach, or not being in proper position to take them, only makes matters worse. **John Reed Stark** walks through the steps CCOS should take to recover quickly and efficiently.

A data breach responder is like a high-tech plumber. Just like a plumber does when a basement floods, data breach responders identify the cause of a breach; combine forces to contain its damage; and collaborate on remediation.

But while a plumber can provide reasonable assurances that the basement will not flood again, a data breach responder cannot promise the same about a future data breach. In fact, another breach is not only possible; it's likely.

That is why data breaches don't define victim companies. How they respond to data breaches does.

Yet while today's news outlets provide an endless stream of data breach reports, rarely is an actual incident response ever discussed. Understanding data breach response workflow not only helps a company prepare for a breach. It also helps a company manage cyber-security risk overall. Below are some of the more typical workflows that companies must undertake amid the incident response of a data breach.

Preservation. Every response to a cyber-attack begins with preservation—that is, collecting and preserving, in a forensically sound and evidentiary unassailable manner, any electronically stored information (ESI) that could become relevant to the investigation of the cyber-attack as well as to the response to any subsequent claims or regulatory demands. Incident responders scrutinize every byte of data, including fragments, artifacts or remnants left by the attacker in remote sectors of devices or systems.

Digital forensics analysis. The most effective cyber-attack investigative methodology is an iterative process of digital forensics, malware reverse engineering, monitoring, and scanning. As analysis identifies any possible indicator of compromise (IOC), investigators examine network traffic and logs, in addition to scanning system hosts for these IOCs. When this effort reveals additional systems that may have been infiltrated, investigators will then forensically image and analyze those systems, and the process repeats itself. Armed with the information gathered during this "lather, rinse, repeat," phase, investigators can detect additional attempts by an attacker to regain access and begin to contain the attack.

Logging analysis. In addition to logs of user systems (like laptop and desktop computers, servers, and so forth), logs of firewalls, intrusion detection systems, and other programs also require preservation and investigation. System logs can record events that occur in an operating system or other software runs, or messages between different users of communication software.

Malware reverse engineering. "Malware" is oft defined as software designed to interfere with a computer's normal functioning, such as viruses (which can wreak havoc on a system by deleting files or directory information); spyware (which can secretly gather data from a user's system); worms

(which can replicate themselves and spread to other computers); or Trojan horses (which upon execution, can cause loss or theft of data and system harm).

The definition of malware, however, is actually broader and a bit of a misnomer, and actually means any program or file used by attackers to infiltrate a computer system. Like the screwdriver that becomes harmful when a burglar uses it to gain unlawful entry into a company's headquarters, legitimate software can actually be malware. Thus, malware reverse engineering is not only an important part of incident response, it's also often the most challenging.

Surveillance. Once a company experiences a cyber-attack, it must "stop the bleeding," and that begins with the installation of surveillance tools. Surveillance means not only performing "full packet capture" (to analyze all traffic passing through a relevant network); but also establishing "alert warnings" to sound alarms when detecting malicious or unauthorized activity.

Remediation. As an investigation progresses, a victim company can use the digital forensics and malware evidence to remediate the malware, rebuild compromised systems, reset compromised account credentials, block IP addresses, and take other steps to improve security. A company will also typically beef up centralized log management; expand its vulnerable management systems; and review its password management. In the long term, a victim company may need to install new hardware and software both for fortification and detection—sometimes even constructing an entirely new network security suite.

EDR Implementation. A common complaint about traditional data breach protection toolsets is that they lack the speed and agility needed to counter sophisticated or clandestine data breaches. So-called endpoint detection and response or "EDR" tools have emerged as the next generation of incident response tools to pick up this slack. Typically installed across an entire IT system or attack vector, the real-time "intelligence feeding" of EDR tools improves a company's ability to detect and respond to outsider and insider threats; enhances a company's speed and flexibility to contain any future attack or anomaly; and helps a company manage data threats more effectively overall.

Exfiltration analysis. Once investigators have determined that an attacker has exfiltrated any personal identifying information (PII) or any other relevant ESI, such as trade secrets, intellectual property, or sensitive e-mail content, a company must begin exfiltration analysis. That becomes an e-Discovery exercise (including hosting relevant ESI). Relevant exfiltrated data can reside almost anywhere, even within programming language or system directories, so searches must be exhaustive, consistent, and scientific. With respect to the more complex datasets, traditional search algorithms and methodologies may not suffice and may require data analytics to carve, parse, and search intricate (and large) company databases.

Physical security evaluation. Physical security and data security are inexorably linked, so data breach response can also entail the review of entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

Regulatory compliance. Responding to state and federal inquiries is a large part of incident response. Privacy laws vary by state jurisdiction, are interpreted unpredictably, and are in a constant state of flux. Some are based broadly, others based on industry sector. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving PII. Federal regulation is a similar mess. Financial and healthcare-related institutions in particular can trigger federal inquiries.

Public companies may also need to disclose to shareholders cyber-risks and cyber-attacks.

Consumer notification and monitoring services. Once a company determines, for example, that PII was exfiltrated, a range of consumer notification responsibilities will arise quickly. This can include the sending of written notices, the provision of credit monitoring services, identity theft protection, and other related services such as setting up a call center, website, hotline, and e-mail address.

Once a cyber-attack occurs, a range of other important notifications arise, such as briefings to customers, partners, employees, vendors, affiliates, insurance carriers, and a range of other impacted parties.

Legal. The work relating to a cyber-attack can involve a team of lawyers with varying expertise (regulatory; e-Discovery; privacy; white-collar defense; litigation; law enforcement liaison; and the list goes on). Potential civil liabilities in the aftermath of a cyber-attack can range from shareholder lawsuits for cyber-security failures or stock price declines to consumer- or customer-driven class-action lawsuits alleging failures to adhere to cyber-security "best practices."

If the digital forensics investigators are retained by counsel, attorney-client privilege will arguably apply to the investigatory work product. This is not done to hide information; rather it helps protect against inaccurate information getting released in an uncontrolled fashion and allows for careful deliberation and preparation for possible litigation or government investigation/prosecution.

Law enforcement liaison. Federal law enforcement agencies will often seek briefings, reports, IOCs, forensic images, malware signatures, and other information about a cyber-attack. They may even ask to attach a recording appliance to a victim company's network in hope of capturing traces of future attacker activity. These requests raise a host of legal issues, including whether providing information to law enforcement could violate the privacy of customers or result in a waiver of the attorney work-product or privilege.

Experiencing a cyber-attack is now inevitable. Cyber-security has become less about prevention and security science, and more about incident response and managing the data breach workflow discussed above. This means that companies should learn from data breach workflow to prepare their incident response now—but how? Here are some recommendations:

- Purchase cyber-insurance (to curtail workflow costs);
- Hire specially trained incident response personnel (to help with tasks such as log analysis, digital forensics, and malware reverse engineering);
- Beef up infrastructure with EDR tools (to assure the most quick and efficient response);
- Data map potentially vulnerable systems, (to make preservation easier);
- Install log analytical programs (to make logging analysis easier); and
- Take other more company-specific preemptive measures to anticipate data breach response workflow, to make it as efficient and inexpensive as possible. ■

A data breach responder is like a high-tech plumber. Just like a plumber does when a house's basement floods, data breach responders identify the cause of a breach; combine forces to contain its damage; and collaborate on remediation.

GET YOUR FREE
CYBER SECURITY AWARENESS KIT

It's a fact: when it comes to cyber security, your employees are your weakest link. Increasing employee awareness of potential threats can minimize your risk.

Get your Cyber Security Awareness Kit at www.navexglobal.com/CyberSecurityKit

NAVEX GLOBAL®

The Ethics and Compliance Experts

Our free Cyber Security Awareness Kit includes useful resources to help educate your employees about how to protect themselves and your organization from cyber attacks.