INSIDE THIS PUBLICATION:

Cyber-Security

Rising to the Challenge

An e-Book publication sponsored by

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 resources for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

HP Security Voltage

HP Security Voltage is a world leader in data-centric encryption and tokenization. HP Security Voltage provides trusted data security that scales to deliver cost-effective PCI compliance, scope reduction and secure analytics. HP Security Voltage solutions are used by leading enterprises worldwide, reducing risk and protecting brand while enabling business. For more information see www.voltage.com.

Inside this e-Book:

Preparing Your Board for Cyber-Security Issues

By John Reed Stark

Every board now knows its company will fall victim to a cyber-attack, and even worse, that the board will need to clean up the mess and superintend the fallout.

Yet 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.

GUEST COLUMNIST

John Reed Stark
President,
John Reed Stark Consulting

So what is the role of a board of directors amid all of 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, 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 periodically 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?

> "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

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 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?

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 instead accepting service of process of multiple subpoenas. The world of incident response is an upside-down one: Rather than being treated like *criminal victims*, companies experiencing data breaches are often treated like criminals themselves, 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. ■

BOARDS SHOW MORE INTEREST IN CYBER-SECURITY

Even among smaller to mid-sized public companies, boards are getting more engaged on cyber-security, with nearly 60 percent of board members in a BDO USA survey saying they are more involved in the discussion now than even a year earlier.

Nearly three-fourths of the 75 board members in the survey said they are briefed on cyber-security at least once a year, and 25 percent said they are briefed quarterly. More than half said their companies had increased the investment in cyber-security in the past year, with the average increase in IT budget reaching 19 percent.

BDO conducted the survey of board members for companies in the revenue range of $250 million to $1 billion to gauge how those companies in that size range are viewing and coping with various issues and trends. Public company boards are not facing any specific regulatory requirement to take up an examination of cyber-security threats, but they are wise to pay closer attention, says Wendy Hambleton, partner in corporate governance at BDO USA.

Board members also reported through the survey that they are starting to hear from management how their companies might consider adopting a new standard on revenue recognition. Slightly more than half of board members said they have been briefed by management on the new standard, and 28 percent said the most difficult aspect of adopting the standard will be updating systems and policies. One-fourth said they expect some issues around revising existing revenue contracts with customers, and 17 percent expect to need to revise debt covenant agreements with financial institutions.

By Tammy Whitehouse

COSO Tacks Toward Cyber-Security Risks

By Tammy Whitehouse

As cyber-security works its way onto the corporate board agenda, COSO is suggesting ways its internal control and risk-management frameworks can be a starting point for companies to anticipate fast-emerging risks.

"One of the key risks we see with cyber-security is that often times the conversation isn't started at the top of the organization," says Sandra Richtermeyer, a COSO board member representing the Institute of Management Accountants. The COSO frameworks give directors and senior management a process for defining and addressing cyber-risks not just within IT, but throughout the organization, she says. "You can't assume all of that's happening in the middle of the organization. It has to start from the top down."

COSO published a paper explaining how companies can manage cyber-risks by assessing and addressing them via the "COSO cube," which is the foundation of COSO's *Internal Control—Integrated Framework*, updated in 2013 to reflect modern business environments. The internal control framework is most familiar to public companies as a way to comply with Sarbanes-Oxley reporting requirements for internal control over financial reporting, but as COSO often points out, its applicability is not limited to financial controls.

In the control environment, for example (the first of the five components of the COSO model), the new COSO paper asks companies to evaluate whether the board of directors understands the cyber-risks and whether they are informed on how the company is managing them. The guidance then walks through the other four components (risk assessment, control activities, information and communication, and monitoring activities) to explain how each area can focus on cyber-security issues and the controls necessary to manage them.

Looking at cyber-risks through the COSO lens allows directors and senior management to communicate their objectives, their view of critical information systems, and their risk tolerances. "This enables others within the organization, including IT personnel, to perform a detailed cyber-risk analysis by evaluating the information systems that are most likely to be targeted by attackers, the likely attack methods, and the points of intended exploitation," COSO says. "In turn, appropriate control activities can be put into place to address such risks."

Mike Rose, a partner at Grant Thornton and co-leader of the GRC practice, says leveraging the COSO internal control framework to assess cyber-risks would give directors a mechanism for overseeing, assessing, and managing cyber risks. "Just as the board is responsible for enterprise risk management, this is very similar," he says.

Considering the proliferation of technology in business, boards have plenty of risks to assess. Rose suggests a company start by identifying its "highest-risk information," which might be anything from intellectual property to customers' personal data. "Then you have to look at the systems and applications storing that information. What are your threats and vulnerabilities?"

Other Paths to Try

Dave Roath, a risk assurance partner with PwC, does see benefit in using the COSO frameworks, but says companies probably shouldn't rely on them exclusively to manage cyber-risks. "No one framework is right for every company," he says.

Roath points to several alternatives: the Framework for Improving Critical Infrastructure Cyber-security, published in 2014 by the National Institute of Standards and Technology; COBIT, a more mature framework for IT governance; and the ISO 27001 and 27002 standards published by the International Organization for Standardization.

"There are so many different elements within a security framework that companies need to worry about," he says. "You need bits and pieces of each of those frameworks to define the risk profile and understand what your crown jewels are."

> "One of the key risks I see with cyber-security is that oftentimes the conversation isn't started at the top of the organization."
>
> Sandra Richtermeyer, Board Member, COSO

Companies have no specific regulatory mandate at this point to use any framework to assess cyber-risks. Hence, the NIST framework was born from an executive order from President Obama in early 2013, and Obama called for more steps to improve cyber-security during his State of the Union address. The Securities and Exchange Commission also requires companies to disclose cyber-security risks (although it doesn't specify how), and indicated cyber-security will be a top concern during its 2015 examination priorities for broker-dealers and investment advisers.

In other words, "There's definitely a focus on setting a tone that says this is a serious risk and it needs to be managed," says Erin Mackler, senior technical manager at the American Institute of Certified Public Accountants.

PwC took the pulse of corporate readiness to do battle with cyber-threats in 2014, and found companies are "all over the board," Roath says. "It's very different based on the industry or sector that a company is in and the size of the company." Companies in financial and defense sectors were more prepared, he said. "They have a much higher degree of spend on security and are much better controlled. Midsize companies tend to be fairly insecure."

Companies are starting to tune into the risks, says Andrew Wallace, a risk assurance partner for PwC. If companies were asked today compared with even a year ago, if they would rate their readiness to withstand a cyber-attack differently, he says. "They would have given themselves a far higher score in the past than they would now, not because they've experienced an event, but because they have seen peers experience these breaches."

Phil Roush, vice president of finance at SanDisk Corp. and vice-chair of a GRC sub-committee at Financial Executives International, says companies that use the COSO frameworks to assess their cyber-risks should take care to assess both the "inside out" and "outside in" risks.

"Inside out deals with employees," he says: namely, how they communicate and what tools they use that might open the door to hackers. Outside-in, meanwhile, "are your vendors, customers, contract manufacturers—all the groups in your ecosystem. How do they get into your network? How do you restrict where they go and what access they have?"

Bill Watts, partner in charge of business risk services at Crowe Horwath, says using a framework like COSO's would let companies still mastering cyber-security take more initiative. "In the past, it's been a very reactive approach to cyber-security, patching leaks in the dam," he says. "The COSO frameworks are broad enough to apply to a lot of different things, including cyber-security. It gives you a formal structure to give people guidance and put a program in place that's proactive." ■

CYBER-RISK ASSESSMENTS

COSO outlines how to use its 17 principles to mitigate cyber-risk.

As an output of the objectives identified as a result of applying Principle 6, an organization should have a clear understanding of the information systems critical to the achievement of its objectives. Applying Principle 7 and Principle 8 then take the risk assessment deeper and lead the organization to assess the severity and likelihood of cyber-risk impacts. When led by senior management, through collaboration with business and IT stakeholders, an organization is positioned to evaluate the risks that could impact the achievement of its objectives across the entity.

To be effective in the risk assessment process, individuals who are involved must have an understanding of the organization's cyber-risk profile. This involves understanding what information systems are valuable to perpetrators of cyber-attacks, and understanding how these attacks are likely to occur. The costliest attacks tend to be the ones that are highly targeted at an organization for specific reasons.

Organizations should be vigilant about understanding their particular cyber-threat profile. Being vigilant means establishing threat awareness throughout the organization and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets. Organizations must incorporate this profile into their overall risk assessment process in order to understand where controls should be placed to keep those assets secure.

It is also important to apply an industry lens to cyber-risks versus just looking broadly at cyber-risks. The perpetrators of cyber-attacks have unique objectives that differ between industry sectors. For example, in the retail sector, organized criminals are the most likely attackers, focused primarily on exploiting vulnerabilities in systems that contain information that can be used for profit (e.g., credit card data or Personally Identifiable Information (PII)). Alternatively, the oil and gas industry might be targeted by nation states with a motive to steal strategic data about future exploration sites. Chemical companies may find themselves targeted by hacktivists because of perceived environmental issues around their products.

Regardless of their motives, cyber-attackers are relentless, sophisticated, and patient. They will stage attacks over time by gathering information that will expose weaknesses within the organization's information systems and internal controls. Through careful evaluation of the motives and likely attack methods and the techniques, tools, and processes (TTPs) the attackers may use, the organization can better anticipate what might occur and be in a position to design controls that are highly effective in minimizing the disruption of potential cyber-attacks and keeping highly valued assets secure.

Change is certain in any organization and should be anticipated in the performance of cyber-risk assessments. The organization will evolve, which includes changes to its objectives, people, processes, and technologies. The cyber-landscape will also change, which includes new perpetrators of cyber-attacks along with new methods of exploitation. While cyber risk assessments are generally reflective of the current state of the organization, the process must be both dynamic and iterative and consider internal and external threat changes that could trigger the need to change how the organization manages its cyber-risks.

Business and technology innovations are adopted by organizations in their quest for growth, innovation, and cost optimization. However, such innovations also create exposure to new cyber-risks. For example, the continued adoption of Web, mobile, cloud, and social media technologies has increased the opportunity for exploitation by the perpetrators of cyber-attacks. Similarly, outsourcing, offshoring, and third-party contracting have exposed organizations to potential cyber-vulnerabilities that are ultimately outside of the organization's control. These trends have resulted in the development of cyber-ecosystems that provide a broad attack surface for the perpetrators to exploit.

The assessment of changes that could have an impact on the system of internal control should include considerations regarding changes in personnel. Turnover of personnel at operational levels of the organization can have a significant impact on the organization's ability to effectively perform their control responsibilities that are designed to minimize the potential impacts of cyber-attacks.

Risk assessments should be updated on a continuous basis to reflect changes that could impact an organization's deployment of cyber-controls to protect its most critical information systems. As information is generated from the vigilant monitoring of the changing threat landscape and the risk assessment process, senior executives and other stakeholders must share and discuss this information to make informed decisions on how to best protect the organization against exposure to cyber-risks.

Source: COSO.

Why Is Cyber-Security a Process? This Is Why.

By Matt Kelly

I recently wrote about how compliance and audit executives might approach cyber-security risks, and foremost was the point that "cyber-security" should be about developing a strong process to govern the information you have, rather than a series of tools and defenses you deploy to keep intruders at bay. Now, I want to revisit that subject from a different angle: from the perspective of the cyber-threat, which is also about developing a strong process to govern the information you have—except that someone else is trying to govern your information, rather than you.

This has been on my mind because I attended the Institute of Internal Auditors' national conference in Las Vegas, and as one would expect, cyber-security risks were all over the agenda. Everyone talking about the subject hammered on two themes. First, as companies move ever further into the world of Big Data—as we automate ever more business processes and create more data—our exposure to cyber-threats will only get worse and worse. Second, the thieves and attackers behind those threats are getting smarter and more agile every day, and right now they're often smarter and more agile than you.

Enough. Those are obvious points, and I'm tired of people making them. We need to step back from the hysteria over our poor cyber-security for a moment and more thoughtfully consider what cyber-threats actually are. Then we can start to find useful strategies in the world of Big Data that compliance and audit executives can use to fight back.

Cyber-threats are about extraction: someone taking information you have and using it for some other purpose. Usually the threat is a thief who wants to extract money and keep it. Sometimes the threat is a thief who wants to extract something of value (credit card numbers, intellectual property) and sell it, or sometimes the threat is an opponent who wants to extract information and expose it, to force you to do something you might not otherwise do, like North Korea hacking Sony e-mails to pressure Sony into canceling "The Interview." In almost every case, however, the activity that happens is extraction.

> We can start to find useful strategies in the world of Big Data that compliance and audit executives can use to fight back.

If extraction is the goal, cyber-threats achieve it by creating a false narrative for the process you have—that is, they lead you to believe that a business process is functioning one way, when actually it is not. They lead you to believe that some wealthy banker in Nigeria needs to wire money into your account, when the banker is a thief in a Lagos café. They lead you to believe the program seeking access to your accounting system is the HVAC maintenance firm looking to submit an invoice, when actually "it" is a gang of thieves in Russia mining their way toward the credit card readers at your cash register. They lead you to believe that Sam in the R&D division wants to see the plans for the new guidance system, when actually they are a front for the Chinese Army. In almost every case, the cyber-threat works by leading you to believe your business process is working one way, when it actually is working another way.

> We need to step back from the hysteria over our poor cyber-security for a moment and consider what cyber-threats actually are.

That point may sound self-evident at first, but the implications behind it are more powerful than many people understand. Why are cyber-risks growing? Because advances in computing technology keep letting us automate more processes, and more complex processes—so we are creating more opportunities for someone to insert a false narrative. In 1965, nobody could impersonate Sam from R&D because Sam physically had to walk to the filing cabinet where the plans were kept, and security guards would recognize him by sight. Now we have automated the human element out of the process. We are doing that more and more every day. When your board asks why cyber-security risks keep growing and when they will stop, that is why they are growing, and they will never stop.

The second implication, however, is that if cyber-threats want to exploit some process you have, in all likelihood they want to do so with stealth—because a business process is something that happens over and over, so the longer the threat keeps mining away at your process, creating a false sense of security, the more benefit it reaps. A good analogy might be the difference between an embezzler who drains a small amount of money away from the company every day, and a robber who grabs $5,000 from the petty cash drawer and then disappears.

You can employ tools to stop the robber, like an armed guard or a security keypad. You need strong processes to stop the embezzler—and make no mistake, the embezzler is a far more difficult enemy for compliance and audit executives to defeat. Because he is chewing away your business processes from the inside every chance he can.

The good news is that the world of Big Data does offer powerful tools and techniques for you to study your business processes and strengthen them for the onslaught coming. Compliance Week will explore those ideas, here in this column and elsewhere in our editorial coverage, for years to come.

But for anyone who hears the talking heads, including me, keep harping that you need to approach cyber-security "as a process" and you quietly wonder what that really means (lord knows I wondered what it meant for a long time), that is what it means—that the threat itself is a process, trying to subvert yours, and the only way to defeat it is to make sure your process is the stronger. ■

Compliance, Audit, and Cyber-Security

The parallels between SOX compliance and cyber-security are deep and vital. A huge amount of cyber-security risk hinges on access

By Matt Kelly

Nobody can get enough guidance about cyber-security these days, and the New England Chief Audit Executives group is no exception. I attended the group's winter meeting here in Boston, and that's all we talked about for two solid hours. These folks had good ideas galore about managing cyber-security risk, so let me recap the most important ones here.

First, worry more about the process of how information is governed at your business than about the tools you use to protect it. The discussion started with a panel of audit and IT executives, and every one of them agreed on this point. Tools address one specific risk, and they may do that quite well—but they may also be useless for every other risk. And if your process for governing information is sloppy overall, those other risks will hit you eventually. The tools you have won't do you much good then.

I always favor analogies from the real world, so try this one: at some point in life you might suffer a heart attack. You can go through life equipped with tools to reduce that risk, such as a defibrillator, and it will indeed help when the time comes. Or you can improve your process of being healthy: eating right and exercising. Neither one of those procedures will assure that you never have a heart attack—but they will help you immensely in staying alive should a heart attack come to pass.

Good tools without good process is the equivalent of carrying around a defibrillator while you overdose on salty foods and sit on the couch all day. Does that sound like a good strategy for preventing heart attacks to you?

Second, define the roles for managing cyber-security risk at your business. Nobody at the CAE group specifically mentioned the Three Lines of Defense model, but that's my default for any conversation about who oversees what part of a risk. In that case, the internal auditors have things a bit easy: You're in the third line as usual, testing the security procedures and controls like you would any other.

The first and second lines of defense get more complicated. Clearly IT (or the IT security function, if you have a separate one) belongs in the second line. Compliance does too. But each one supports the business units bravely holding down the first line of defense in different ways. My first point above, to worry more about process than tools, still holds true—but you do need both tools and process to have effective cyber-security: IT supporting the tools to fight cyber-security risks, compliance supporting the processes.

I like to think of effective cyber-security defense as this: for business units to follow effective processes there in the first line, compliance needs to do its job in the second line defining what those processes are. They might be policies to have third parties certify their data security, or procedures for swift disclosure of a data breach. But the business units can't follow a good process unless compliance does its job spelling out the policies and procedures that govern that process.

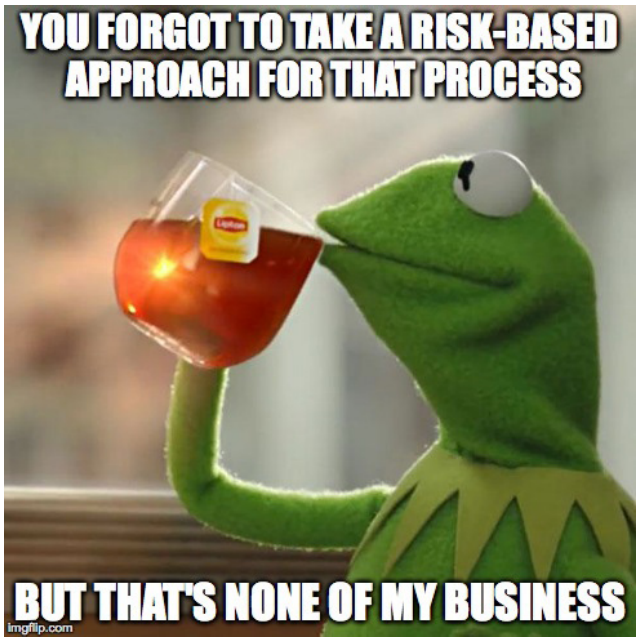
The third point I heard, and perhaps the most heartening one, was that Corporate America has faced a mess of poor controls and poor understanding of risk before—and we solved the problem. We've been here before with Sarbanes-Oxley compliance.

Numerous times I heard speakers worry about weak processes and then breezily add, "unless it's a SOX process, because our SOX processes are generally strong," or "If it's a SOX-related control usually we're confident it works."

Study those parallels between SOX compliance and cyber-security, because they are deep and vital. A huge amount of cyber-security risk hinges on access: ensuring that only authorized users get access to certain types of data. That is the same worry compliance and internal auditors have about access control to financial information—and you've been testing your access controls for financial data for the better part of a decade. Drop the word 'financial' from my last sentence, and you have your marching orders for cyber-security risk. I'm not saying that goal is easy to achieve, but that's the goal.

You can even make an intellectual leap from SOX compliance back to the importance of a strong process. When you read through the 17 guiding principles of the updated COSO framework—the framework we're all using for SOX compliance—those principles are all about strengthening your process. Everyone might be using the framework right now for internal control over financial reporting, but COSO intended the framework to be a roadmap for internal control over other risks too, cyber-security included.

So as scary as cyber-security might be right now, it can be conquered. If the compliance and audit community tamed Sarbanes-Oxley, you're in prime fighting shape for this threat too. ■



Streamlining Information Protection Through a Data-centric Security Approach

Overview

The sophistication and persistence of criminal attacks on online systems is growing, along with government regulations requiring full disclosure for breaches. The potential compromise to business brand, reputation, and revenues means that data security is no longer optional, but is essential for customer retention and business longevity. Regulatory and compliance requirements bring additional urgency for the need to protect sensitive data.

To date, data protection through encryption, tokenization, and masking have been complex and tedious processes. Application and process development is highly complex, IT administration is cumbersome, and projects can take enormous resources and time to complete. With complexity comes risk. Despite technologies being available for many years, database encryption is the exception rather than the rule. Some firms still use high-risk production data in test or outsourced environments. An alarming number of data thefts from breaches have occurred as a result of data exposed in both production and non-production environments.

HP Security Voltage introduces a unique approach that combines data encryption and masking technology in one, which can vastly simplify data privacy, while mitigating data leakage at a fraction of the cost of prior approaches. One fundamental technology is HP Format-Preserving Encryption (FPE), which for the first time, allows encryption 'in place,' in databases and applications, without significant IT impact. Another technology is tokenization, which replaces data with random tokens and which can also preserve data formats. These technologies are integrated with masking techniques on the HP SecureData Platform, allowing projects that once lasted months or years to complete in days to weeks.

HP SecureData offers a consolidated approach using the above technologies, replacing multiple point solutions with a platform that is agnostic of data storage and operating systems, including convenient delivery and integration options. Both contemporary and legacy enterprise IT systems are readily accommodated, speeding compliance with regulations and standards. Applying HP SecureData to protect credit card data, for example, can dramatically reduce PCI DSS compliance scope and audit costs. This document covers the use of HP FPE and HP Secure Stateless Tokenization (SST) for field-level data protection, as well as both static and real-time data masking.

Why Data Needs a New Approach to Protection

In an ideal world, sensitive data travels in well-defined paths from data repositories to a well-understood set of applications. In this case, the data can be protected by armoring the repository, the links, and the applications using point solutions such as transparent database encryption and SSL network connections.

In real systems, data travels everywhere. Today's IT environment consists of a constantly shifting set of applications running on an evolving set of platforms. In large enterprises, the data lifecycle is complex and extends beyond the container and application, sometimes outside traditional enterprise IT departments into places like offsite backup services, cloud analytic systems, and outsourced service providers. For transactions involving personal and payment identifiers, many applications must be coordinated to protect the data.

This means that armoring the repositories, applications, and links doesn't provide the needed protection, because the data won't stay in one place. Even if you could manage to keep up with the rapid changes in infrastructure by installing and managing security solutions from a wide range of vendors, you will have security gaps in between the armored repositories, applications, and links. For example, data is exposed after it is decrypted and retrieved from a transparently encrypted database and before it flows through an encrypted link, leaving it vulnerable to an attack. Consequently, legacy security solutions have failed to deliver and have been removed, bypassed, or applied unevenly in many businesses. The results could not be clearer: Breaches involving unprotected business and customer data are front page news almost every day, with disastrous consequences.

The following illustrates the weakness of conventional approaches to data protection:

WHOLE DATABASE ENCRYPTION

- Encrypt data within DB - slows all apps down
- No granular access control
- Separate solution for each database vendor
- No separation of duties - DBA can decrypt
- No security of data within applications and networks

DATABASE COLUMN ENCRYPTION

- Encrypt data via trigger and stored procedure
- Require schema changes
- No data masking support or separation of duties

NATIVE OR TRADITIONAL APPLICATION-LEVEL ENCRYPTION

- Encrypt data itself, throughout lifecycle
- Requires DB schema/app format changes
- Heavy implementation cost

SHUFFLING

- Shuffle existing data rows so data doesn't match up
- Breaks referential integrity

» Can still leak data

DATA TABLES AND RULES

» Consistently map original data to fake data
» Allows for referential integrity, reversibility
» Security risks due to use of look-up tables

WEAK, BREAKABLE ENCRYPTION

» E.g., stream ciphers, alphabetic substitution
» Not secure - easily reversible by attacker
» Key management challenges

The Data-centric Approach

HP Security Voltage has pioneered technology that protects data independent of the subsystems that use it. HP Security Voltage products can protect sensitive data as soon as it is acquired and ensure that it is always used, transferred, and stored in protected form. Selected applications decrypt the data only at the time that it is processed, while others work with encrypted or masked data.

HP Security Voltage provides two technologies for protecting data: HP Format-Preserving Encryption (FPE), and HP Secure Stateless Tokenization (SST). These independent methods are proven to protect data while preserving data format and other attributes, effectively building the protection into the data itself. Replacing the original data with either an encrypted value or a random token narrows the possible exposure of data and can greatly reduce audit scope and compliance costs.

Demands of Data Protection in Existing Systems

There are special demands that must be met when implementing a data protection solution that leverages existing systems without major disruption.

The first demand is referential integrity. It is common that the same identifying data is present across multiple databases and application systems. Applications depend upon the pervasiveness of common identification data, such as credit card numbers or social security numbers (SSNs). These data must be stored with consistent values to allow matching across databases.

It is a challenge to maintain referential integrity in encrypted data. Consider an example with three separate databases (potentially on different platforms), using common data such as SSN to access records in the database. If we encrypt one database's SSN field, then we have lost referential integrity across the different databases, as the encrypted SSN field will appear as random binary data. The databases and applications will lose the ability to link and index tables using the SSN, causing operational failure. Therefore data protection must be coordinated across databases. The data inside the database must be consistent, providing unique identifiers, so that data can be linked before being presented to applications.

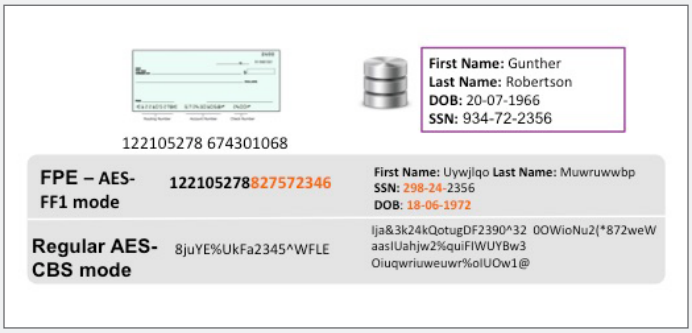
Another demand of data protection in existing systems is format preservation. Identifiers have specific formats, with definite lengths, and sometimes, punctuation. Applications are written with these formats built into their code base in many areas—the definitions of variables, the allocation of temporary space, the layout of user interfaces, etc. When protecting data, it is critical that the format of the original data be preserved; otherwise applications would have to be re-written and processes may have to be changed, at great expense. The HP SecureData platform provides four techniques that can be combined to meet the demands of data protection in any setting. These are encryption, tokenization, static data masking, and real-time data masking.

HP Format-Preserving Encryption

HP SecureData provides HP FPE using AES-256 encryption. HP FPE combines a novel, published method (see FFX Encryption Mode on the U.S. Government NIST website) with an existing, proven encryption algorithm (AES) to encrypt data in a way that does not alter the data format. Like traditional AES, the HP FPE algorithm uses strong 256 bit keys, and like AES, with the ciphertext and the original key, an application can get back the unencrypted value. A variation of this technology allows the identity and access policy data to be embedded within the cipher text.

The fact that the encrypted value has the same size and data format as the original enables HP FPE to be used with little or no changes to database schemas and applications. And inherent to how HP FPE works, when encrypted values are transported from mainframes to open systems, no EBCDIC to ASCII conversion is required.

HP Format-Preserving Encryption (FPE)



HP Secure Stateless Tokenization

HP SecureData also provides tokenization. Tokenization replaces data values with a "token" or random string of text. HP Secure Stateless Tokenization (SST) technology is an advanced, patent pending, data security solution that provides enterprises, merchants, and payment processors with a new approach to help assure protection for payment card data. HP SST technology is "stateless" because it eliminates the token database, which is

central to other tokenization solutions and removes the need for storage of cardholder or other sensitive data. HP Security Voltage has developed an approach to tokenization that uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual "appliances"—commodity servers —and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with SST technology, thus improving the speed, scalability, security, and manageability of the tokenization process. Tokenization has a special advantage for credit card numbers: The PCI DSS guidelines consider systems that only hold tokens to be out of audit scope, greatly reducing audit costs.

In HP SecureData, the tokens have the same format as the original data, gaining all the advantages of FPE. Specifically, both FPE and HP SST have the following properties:

» Format can be exactly preserved, such as a nine-digit SSN becoming a nine-digit token, or it can be altered, such as a 16-digit credit card number becoming a 16-character string with some digits replaced by alpha characters—to assist auditors in immediately recognizing the difference between a token and a real credit card number.

» They are deterministic, which means that the same input, encrypted or tokenized twice, will result in the same output. This feature enables preservation of referential integrity, without the need to keep an application-specific reference database.

» Because they are reversible, they guarantee against collisions (for each input, there is one and only one output, and vice-versa).

HP Security Voltage products can protect sensitive data as soon as it is acquired and ensure that it is always used, transferred, and stored in protected form. Selected applications decrypt the data only at the time that it is processed, while others work with encrypted or masked data.

Static Data Masking

The properties of FPE described above can also be employed to generate test data based on production data. The process of converting a production data set into de-identified test data is called "static data masking." FPE can be configured for both reversible and non-reversible data masking. In reversible mode, the encryption key is centrally generated and managed, allowing recovery of the original data when required. In a non-reversible or one-way mode, an ephemeral encryption key is randomly generated for each encryption and subsequently thrown away. Both techniques can be useful for QA test data. Reversibility is important in scenarios such as:

» Medical researchers need "blind" data but occasionally an actual patient's identity must be uncovered by an authorized person.

» Trading partners require a subset of test data, in original clear text form.

» A problem occurs in production but cannot be reproduced with masked data.

In the past, masking processes would lose relationships across databases, would be very complex to manage with special rules or tables, or would require substantial storage as lookup tables as large as the original databases were required. Thus, additional terabyte SANs were required just for storage of masked datasets. FPE provides static data masking capabilities without the large lookup tables filled with sensitive data that are used in traditional data masking solutions.

Different applications have different data needs. HP SecureData supports a powerful feature, run-time data masking, which allows different applications to meet their information needs with a run-time choice of data mask. Data is only exposed on a "need-to-know" basis. Credit card numbers provide a good example. Analytics users do not need the original numbers, but they do need unique identifiers or tokens that are used consistently. Customer Relationship Management (CRM) users may need only the last 4 digits of the actual number with the other digits masked. Only final payment processing systems and fraud auditors need the original unencrypted data. In effect, each application sees the data through its own specific mask, allowing for very precise control of data security.

Conclusion

Compared to past approaches HP SecureData offers distinct advantages. In addition to the security advantages of HP FPE and HP SST, integration efforts are reduced to hours and days, instead of months or years as in the past. De-identification of data for testing or other purposes leverages the same data protection used in production. As a true enterprise platform, clients can start with simple applications and expand the use of HP SecureData across any number of applications and systems, from HR to financials to custom applications to integration with CRM and Enterprise Resource Planning (ERP) systems. The same platform can be re-used for bulk unstructured data handling with HP SecureFile and HP SecureMail, for enterprise-wide data privacy and complete peace of mind.

The bottom line is that data protection is now feasible across the enterprise with a single approach. HP SecureData offers huge reductions in cost and time for privacy compliance. The data-centric approach mitigates data leakage and avoids disclosure from the outset, regardless of platform choice, outsourcing needs, scaling requirements, or IT processes. For the first time, information protection and database security are simple and easy to implement, becoming a natural extension of existing infrastructure and processes.