Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Fortifying your Cyber-security efforts

An e-Book publication sponsored by RSA

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. http://www.complianceweek.com

RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to rsa.com.

Inside this e-Book

Getting ready for SEC cyber-security tests

The SEC is testing investment firms for cyber-security readiness. Preparing is a marathon, writes **Eldon Sprickerhoff**, not a sprint.

Governments will eventually regulate industry to solve ongoing problems, and the investment industry is no exception. As cyber-risks increasingly threaten corporate finance, the Securities and Exchange Commission is tightening controls to ensure that registered investment advisers and funds comply. Here's what's happening and what you must do about it.

The SEC began looking at cyber-security in the financial sector as early as 2011, when it published a guidance document on the disclosure of cyber-security risks for corporate finance. This was an opinion, though, rather than an enforceable rule.

It ramped up its coverage of cyber-security risk in March 2014, holding a Cyber-security Round Table with market participants, and followed this up by announcing cyber-security examinations for registered investment advisers a month later through its Office of Compliance Inspections and Examinations (OCIE).

After a "security sweep" on 50 RIAs that September, the SEC issued a guidance update through its Investment Management Division in 2015. This document warned of periodic assessments and asked

companies to produce a strategy for preventing, detecting, and responding to cyber-security threats.

As the SEC developed its cyber-security policy, it gained teeth. When RT Jones Capital Equities Management failed to produce a written security in September 2015, the regulator fined it $75,000 under Rule30(a) of Regulation S-P, commonly known as a the "safeguard rule." This rule mandates that participants maintain written policies and procedures for protecting customer data. It's important to note that while being slapped with a fine reflects poorly on a firm, it's the reputational damage done by SEC disclosure that's more harmful.

Since then, the SEC has increased its focus on cyber-security. In 2016, then-SEC Chair Mary Jo White warned that financial partners are still not tailoring policies and procedures to their specific risks. The regulator performed a cyber-security sweep of funds; broad findings are expected to be released this year.

This aggressive approach to cyber-security regulation should give companies pause in 2017. The OCIE recently published its examination priorities for the year, highlighting cyber-security as a focal point.

"In 2017, we will continue our initiative to examine for cyber-security compliance procedures and controls, including testing the implementation of those procedures and controls," the OCIE said.

Preparing for the future

There are six measures compliance professionals in financial services should consider when working to comply with these regulatory requirements:

- **Understand the digital assets under your care.** Companies should be aware of the most critical sensitive data that they hold.
- **Perform a risk assessment.** Once companies understand the data that they are responsible for protecting, they can explore the risks that may expose it. There are some that they can mitigate, such as storing it in a cloud-based service, for example. Then, there are others that companies can offset through insurance. Finally, there are some risks that financial firms may simply have to accept.
- **How you secure the assets.** This will be the most significant and time-consuming of the six steps and involves a detailed technical exploration of the tools and techniques necessary to protect the assets under management. The level of risk that different assets face will be an important consideration.
- **Run periodic vulnerability assessments.** Cyber-security is not a one-time, "fire and forget" project. It is a living, breathing process that advisers and funds must revisit as both threat vectors and business conditions change. Conduct regular vulnerability assessments to ensure that you are still adequately protecting yourself against risks.
- Based on those assessments, you will need to complete two more steps:
    - **Tighten security policies.** Vulnerability assessments may highlight new risks that need an adjustment in security policy. This is part of the regular cycle of risk assessment and mitigation.
    - **Conduct awareness training.** After they put technical controls and security policies in place to secure their assets, investment firms must acknowledge the other weak spot: people. Training staff to support security policies is an important part of this six-step process.

Firms must put these steps in place and document them. They should not underestimate the work involved in this process. It is not unheard of for some firms to devote three people to the process for two months to prepare for an SEC examination.

On the upside, putting in this work to follow the SEC guidance will get companies a long way toward compliance with regulation from other relevant bodies. FINRA produced its own *Report on Cyber-security Practices*, which it expects companies to follow.

The level of work required for regulatory compliance, combined with the need to keep current with evolving cyber-security risks, makes this a marathon and not a sprint. Devoting the human resources to cope with the workload is only half the battle; the other half involves developing a cyber-security mindset and making it a part of your culture. ■

Choosing a sound path forward for cyber-security

When it comes to cyber-security risk management, let's pursue a flexible, principles-based approach—and avoid a road to nowhere paved with layers of compliance rules. **Cindy Fornelli** reports.

Capital market stakeholders across the spectrum are as primed as ever to take action on an issue that affects us all: cyber-security. Fifty percent of U.S. CEOs say they are "extremely concerned" about cyber-threats, according to a recent survey by PwC. Boards of directors are engaged on the issue, while investors overwhelmingly perceive cyber-security attacks as one the biggest risks to their portfolios. For policymakers at home and overseas, cyber-security continues to climb the list of priorities.

This rising cyber-awareness is necessary and fitting, given the urgency of confronting cyber-security threats and the astonishing aggregate cost of today's cyber-attacks. Yet, as momentum picks up, we must carefully consider our overall approach to cyber-security risk management—there are several possible paths ahead. Moreover, cyber-security is particularly challenging terrain, given its complex and shifting nature. Organizations face varying threats and actors, all in the context of relentless and rapid

technological change.

So, which path should we choose through this difficult landscape?

First, our approach to cyber-security risk management should be principles-based, setting the focus on an end result and letting the private sector bring to bear its agility, energy, and innovation to achieve that result. For cyber-security, one critical objective should be enabling companies to establish robust cyber-security risk management programs that are tailored to their particular situations, needs, risk appetite, and threats faced.

Yet, accomplishing that objective becomes increasingly difficult if overly prescriptive regulations or standards force companies to meet a raft of requirements that align poorly with their businesses and risks. At that point, cyber-security risk management devolves into a burdensome compliance exercise, one in which merely checking boxes becomes a resource-draining end, a path we should avoid.

Second, a sound approach to cyber-security should build on and leverage the good work that has already been done in this area. Several organizations have developed cyber-security management frameworks—such as those put forward by the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST)—to help organizations manage cyber-security risk.

Third, we need to incent positive action. Companies should be rewarded for making good faith efforts to protect against cyber-security breaches, to detect cyber-threats and to remediate in a timely manner following a breach.

While a broad-based consensus may not have formed around the three-point approach outlined earlier, there has been promising movement in that direction. Recently, the American Institute of CPAs (AICPA) unveiled an entity-level cyber-security reporting framework through which organizations can communicate useful information about their cyber-security risk management program to a broad range of stakeholders, including boards of directors, senior management, investors, and others.

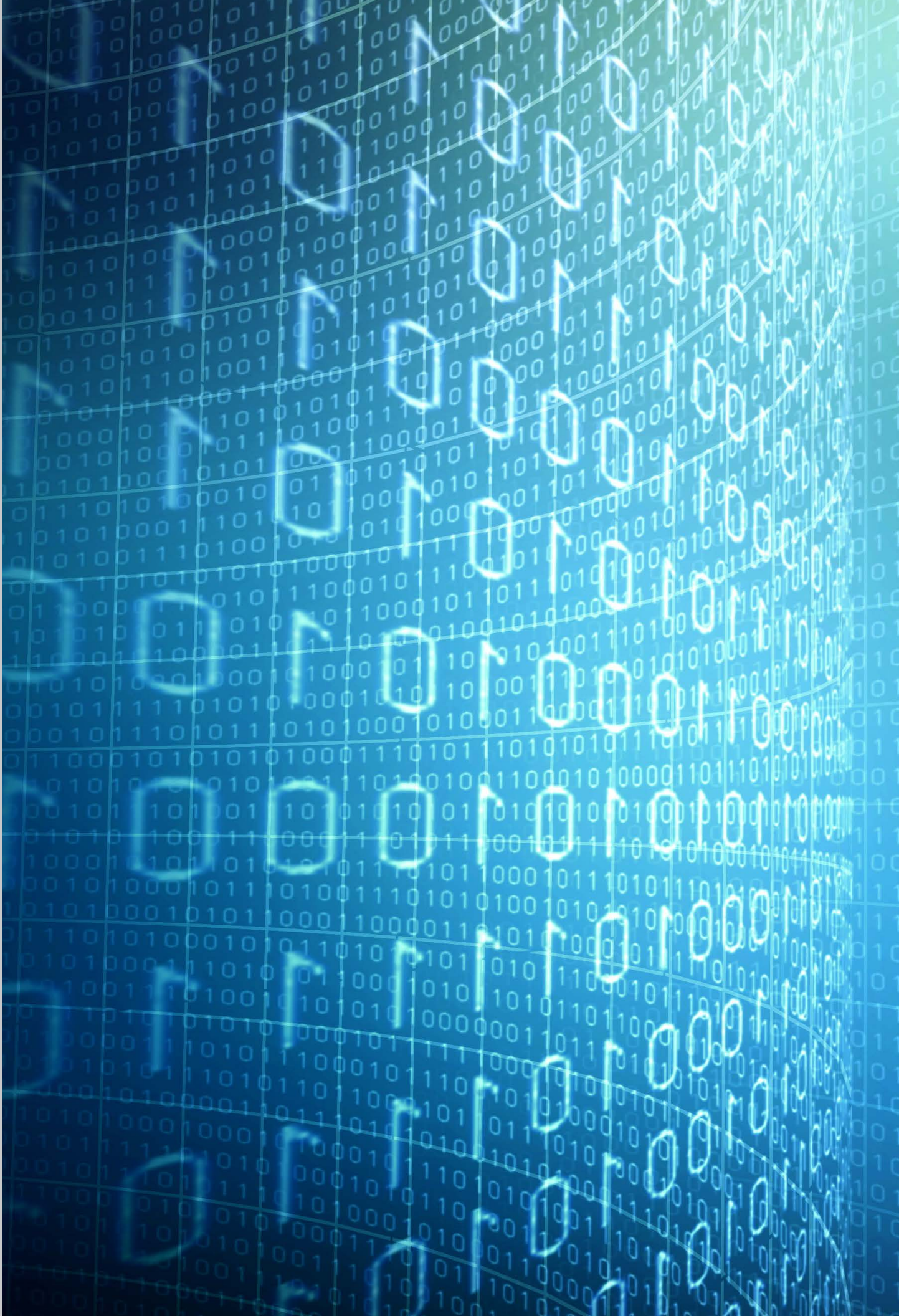
The AICPA's reporting framework has three key components: The first is Management's Description of the entity's cyber-security risk management program, based on suitable criteria. The second is Management's Assertion to the presentation of their description and to the effectiveness of controls implemented to achieve the entity's cyber-security objectives. Finally, the AICPA framework includes a CPA's Opinion on that description and the effectiveness of the controls to meet the entity's cyber-security objectives.

The AICPA's reporting framework is principles-based and voluntary, and companies do not need to implement all three of its components at once. Rather than prescribing specific requirements, its description criteria set forth the types of policies and procedures that companies can adopt for cyber-security risk management. With the aid of the criteria, companies can decide what works best for them.

What's more, the AICPA framework leverages existing cyber-security and risk management structures. It maps to commonly used cyber-security risk management frameworks—such as NIST and ISO—and aligns to the 2013 COSO Internal Control - Integrated Framework so cyber-security can be integrated with companies' broader enterprise risk management efforts.

Finally, and no less important, the AIPCA approach incents companies to take action. While the framework cannot guarantee against cyber-attacks, it offers companies the benefit of an independent, objective opinion on their cyber-security risk management. In addition to bolstering the company's own confidence, that independent opinion can provide decision-useful information to other key constituencies, including directors and investors.

The AICPA's cyber-security risk reporting framework is a step toward harnessing the power of the private sector, making the most of existing resources, and increasing the confidence of investors and other stakeholders. It represents progress down a sound path forward for cyber-security. ■



Data breach trends industry-by-industry

The 2017 Verizon Data Breach report is out, and it has some timely pointers for how healthcare, financial services, manufacturing, and retail organizations can improve their cyber-security procedures. **Jaclyn Jaeger** has more.

Cyber-security has become a major compliance issue in recent years as the frequency and severity of data breaches and information security incidents has prompted organizations to direct all available resources to deal with the problem.

To help companies in their efforts, *Verizon's 2017 Data Breach Investigations Report* takes a deep dive into 1,935 breaches and 42,068 security incidents from 65 contributing organizations. In the report, Verizon defines "incident" as "a security event that compromises the integrity, confidentiality or availability of an information asset" and defines a "breach" as "an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party."

"The majority of breaches are financially motivated and somewhat opportunistic in nature," Mark Spitler, the report's lead author, said in a Webinar discussing the results. "I don't expect that to go away any time soon." Specifically, 73 percent of breaches were financially motivated, while another 21 percent were the result of cyber-espionage carried out by state-affiliated actors.

An assessment of data breach trends by industry based on data in the Verizon data breach report—including who carries them out, how they are carried out, and what companies can do to mitigate the risk—is discussed in more detail.

Healthcare. Whether caused by an internal or external threat, data breaches plague healthcare organizations more than any other industry. Insider misuse is especially problematic, with healthcare being the only industry in which employees are the predominant threat actors in breaches.

The specific motives behind breaches caused by internal actors are almost equally divided between financial motivations (identity theft) and fun (employees accessing patient data out of curiosity—for friends or relatives, for example).

Carelessness is another significant issue in the healthcare industry. Delivering healthcare records to the wrong patient, disposal errors, and lost documents made up another 30 percent of healthcare breaches.

It's upsetting to continue to hear about unencrypted laptops resulting in a breach disclosure, Spitler said. "It's not going to get your laptop back," he said, "but it can prevent you from having to say, 'We just lost a thousand patient records.' "

The Verizon report recommends several measures healthcare organizations can implement to mitigate the risk of a breach or incident:

- Have a process that requires a second individual to sign off on any online changes to avoid publishing errors;
- Have a policy in place for disposal of any personally identifiable information (PII), and make sure that it is monitored for compliance;
- Encrypt all mobile devices to limit the impact of lost or stolen devices;
- Routinely check employee activity to ensure they are not viewing, downloading, or printing information that they have no business need for;
- Use warning banners, making it clear to employees that their data use at work is being monitored; and
- Where feasible, tokenize sensitive information—such as Social Security Numbers—when used to identify a record that the employee does not need for billing purposes or patient care.

Ransomware—when attackers encrypt the contents of a device and then demand a ransom to unlock the data—is another top cyber-threat facing healthcare organizations. This is because electronic health records—rich in credit card data, Social Security Numbers, employment information, and medical records—fetch a high price on the black market.

In the Verizon report, ransomware attacks were not counted as breaches because of the inability to confirm that data confidentiality was violated, the report explains. Guidance issued by the Department of Health and Human Services, however, recommends that healthcare organizations treat ransomware as a breach for reporting purposes. In the event of a ransomware attack, the Verizon report recommends backing up all systems routinely and have them ready to fall back on.

Financial and insurance. In the financial services industry, 88 percent of incidents resulted from denial-of-service (DoS) attacks; Web app attacks; or cyber-espionage, the Verizon report finds. Ninety-six percent of these attacks were financially motivated—such as accessing systems to fraudulently transfer money or using the personal information of customers for identity theft.

The Verizon report defines a DoS attack as "any attack intended to compromise the availability of networks and systems." This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

One way to minimize the risk of a DoS attack is to "have a DoS protection and mitigation service in place and make it your job to know the details of the agreement with the provider," the report states. Additionally, the report recommends using two-factor or multifactor authentication to help secure all Web applications.

"Not all industries are going to be affected by the same threats with equal frequency," Spitler said. In the financial services industry, for example, insurers and investment bankers do not have to worry about credit card skimmers in the same way that commercial bank or credit unions do.

After taking ATM skimming, DoS, and botnets out of the equation, the Verizon report found privilege misuse to be the most common incident pattern within select financial industry breaches. Thus, it's a good idea to "keep an eye on employees, and periodically monitor their activities," the report advises. "Do not give them permissions they do not need to do their job, and make sure you disable accounts immediately upon termination or voluntary departure."

Another important measure: Keep audit logs of user activity not just to hunt down malicious or inappropriate users, but also to prevent external adversaries from gaining access using legitimate internal credentials, Spitler said. The same security controls designed to identify employee misuse can also detect external attackers masquerading as privileged users.

Retail. In the retail industry, 81 percent of 209 hacking incidents resulted from DoS attacks; Web app attacks; and payment card-skimming attacks.

A Web app attack is where a Web app—such as a content management system or e-commerce platform—is used as a means of entry. Breaches involving e-commerce sites, for example, typically involve hacking the Web application, with credentials stolen from customers as part of phishing attacks being the predominant method of Web app compromise.

Traditional storefront retailers must contend with an entirely different threat vector: the installation of card skimmers inside gas pump terminals, ATMs, or point-of-sale (PoS) terminals. These devices account for almost 60 percent of non-e-commerce retail breaches.

"Using default or easily guessable passwords simply will not cut it in today's world," the report states. "Implement multifactor authentication across your enterprise but especially for remote access into payment card processing networks."

Manufacturing. In the Verizon report, cyber-espionage comprised most breaches within this industry, resulting in 108 out of 124 breaches. Most

of these breaches were conducted by state-affiliated actors, but instances of internal espionage pilfering trade secrets were present, as well, the report states.

Many of these attacks are financially motivated. In fact, a whopping 90 percent of data stolen in manufacturing targeted valuable corporate data—such as intellectual property, trade secrets, or other sensitive information.

Unique to the manufacturing industry is how long these attacks are carried out. Typically, criminals infiltrate the network, locate the sensitive data, and then lurk in the shadows siphoning the data as long as possible. Malware gets onto a company's system, for example, when someone clicks on a malicious e-mail or visits an infected Website.

> "Not all industries are going to be affected by the same threats with equal frequency."
>
> Mark Spitler, Lead Author, Verizon's 2017 Data Breach Investigations Report

Privilege misuse, which occurred in just eight instances in the manufacturing industry, made up the second most common incident pattern, the report found. Typically, privilege misuse occurs when a disgruntled employee leaves a company with sensitive corporate data.

To prevent cyber-espionage, the Verizon report recommends the following proactive measures:

» Keep highly sensitive data segregated, and only allow access to those who require it to perform their job;
» Train employees about phishing scams, and provide them with a quick and easy way to report suspicious e-mails;
» Monitor internal networks, devices, and applications; and
» Implement data-loss prevention controls to identify and block improper transfers of data by employees.

Hospitality industry. Among hotels and restaurants, PoS attacks dominate. Ninety-six percent of breaches involved external actors, with 96 percent carried out by financially motivated organized criminal groups, the Verizon report states.

The hospitality industry is particularly vulnerable to malware attacks, representing 94 percent of breaches in 2016. "Malware is not going anywhere," Spitler said. Most companies—even outside the hospitality industry—have some level of anti-virus software, but they need to be thinking bigger, he said.

The Verizon report recommends, for example, filtering remote access to PoS networks and only allowing connections from whitelisted IP addresses. It is also important to "patch promptly and consistently and make certain all terminals and servers are running the most recent version of software," the Verizon report states.

Across all industries, the gap between the time it takes for a cyber-criminal to compromise a system and the time it takes for an organization to discover a breach is still significant. Thus, companies should focus their efforts on both making it more difficult for intruders to exit the system once they have broken into it and improve the speed with which a breach can be detected, Spitler said. Although companies will still have to deal with a data breach or security incident, he said, "the impact will be much less."

The goal of Verizon's data breach report is to arm companies with the knowledge they need to defend against these incidents, said John Loveland, global head of cyber-security strategy and marketing at Verizon. "We see the market shifting to intelligence-lead solutions, leveraging threat intelligence to make better decisions about how to allocate resources from a cyber-security perspective, as well as how to anticipate, prevent, and respond to cyber-breaches when they occur." ■

CYBER-ATTACKS ACROSS INDUSTRIES

Below is a list of companies from various sectors that fell victim to cyber-attacks in 2016.

Healthcare. *Hollywood Presbyterian Medical Center ransomware attack.* In February 2016, Hollywood Presbyterian Medical Center disclosed that it had experienced a malware attack earlier that month, which temporarily affected the operation of its computer network. The malware locked access to certain computer systems by encrypting files, preventing hospital staff from sharing communications electronically. To make matters worse, the hackers demanded ransom to obtain the decryption key—40 Bitcoins, or approximately $17,000, to be exact. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Hollywood Presbyterian Chief Executive Officer Allen Stefanek said in a statement.

Financial services. *SWIFT data breach.* The Society for Worldwide Interbank Financial Telecommunication (SWIFT), a member-owned cooperative, disclosed in August 2016 in a private letter to its members that it had uncovered yet more cyber-theft attempts on its member banks. The discovery followed the $81 million heist at Bangladesh Central Bank in February 2016. "Customers' environments have been compromised and subsequent attempts [were] made to send fraudulent payment instructions," read a copy of the letter reviewed by Reuters. "The threat is persistent, adaptive and sophisticated, and it is here to stay."

Manufacturing. *FACC data breach.* FACC, an Austrian-based aerospace parts make—with clients including Airbus and Boeing—announced in January 2016 that it had fallen victim to hackers. Rather than go after the company's data and intellectual property, the criminals stole approximately €50 million (US$54.5 million) in funds.

Accommodation and food services. *Wendy's data breach.* In May 2016, fast-food chain, Wendy's, said in a securities filing that malware, "installed through the use of compromised third-party vendor credentials, affected one particular point of sale system at fewer than 300 of approximately 5,500 franchised North America Wendy's restaurants, starting in the fall of 2015." Wendy's continued: "The company has worked aggressively with its investigator to identify the source of the malware and quantify the extent of the malicious cyber-attacks and has disabled and eradicated the malware in affected restaurants." HEI Hotels and Resorts breach. In August 2016, HEI Hotels and Resorts, which operates 20 hotels across several well-known hotel chains, reported that its payment system had been breached. Affected properties included several Starwood's Westin hotels, as well as several Starwood and Marriott properties. HEI said that unauthorized individuals installed malware on its payment processing systems at these affected properties enabling them to capture payment-card information at the point of purchase.

Retail. *Eddie Bauer malware breach.* In August 2016 (just weeks after HEI disclosed its breach), retail chain Eddie Bauer informed its customers that it had discovered that point-of-sale-systems at Eddie Bauer retail stores may have been accessed without authorization. Upon detecting the issue, the company engaged third-party digital forensic experts to investigate. That investigation determined that customers' payment card information used at Eddie Bauer retail stores on various dates between January 2016 and July 2016 may have been accessed.

—Jaclyn Jaeger

Data privacy considerations in M&A deals

The increasingly ominous specter of cyber-risk can cast a shadow over any merger or acquisition. But due-diligence practices can lower the risk. **Jaclyn Jaeger** has more.

Data privacy and cyber-security risks play an increasingly prominent role when evaluating a potential corporate merger or acquisition target. Knowing how to manage these risks could mean the difference between a smooth M&A transaction and one that quickly turns into a liability nightmare for the buyer.

Verizon's acquisition of Yahoo in February 2017 provides a recent, high-profile example. Verizon ultimately decided to move forward with the acquisition, even after discovering that Yahoo had suffered two massive data breaches, compromising over one billion user accounts.

In a Feb. 21 filing with the Securities and Exchange Commission, detailing an amended deal, Verizon said Yahoo will retain 50 percent of "certain post-closing liabilities arising out of governmental or third-party investigations, litigations,

or other claims related to certain user security and data breaches." Additionally, Yahoo will continue to be held fully liable for liabilities arising out of any shareholder lawsuits, as well as any SEC investigations and actions.

Some have questioned whether Verizon would have uncovered Yahoo's data breaches if it had done more robust due diligence, a claim that Craig Silliman, Verizon's general counsel, disputes. "There is no way you can do due diligence and find something ... that the company itself hasn't found," Silliman told *Corporate Counsel*.

"I don't think one of the lessons learned is the need for due diligence around data breaches," Silliman added. "I do think it points to the importance of reps and warranties around data breaches."

One benefit of having representations and warranties in a purchase agreement, as so clearly demonstrated by the Verizon-Yahoo deal, is to proactively address risks and cover any potential gaps not found in the due-diligence stage. "We are seeing the development of quite robust reps and warranties in the areas of data privacy and cyber-security," said Joshua Rawson, a partner and leader of the U.S. Technology and Intellectual Property Transactions practice group at law firm Dechert, which hosted a Webinar addressing cyber-security considerations in M&A transactions.

Data-privacy and cyber-security considerations in M&A transactions are a developing area. Some representations focus on ownership of the data, for example, and the ability to transfer data to the buyer without violating laws or contracts, Rawson explained. Other reps and warranties call out specific types of laws that the buyer may be concerned with and wants the seller to take ownership of, including European data protection laws, he said.

Other representations in a purchase agreement address the sufficiency of security measures and backup disaster recovery measures; existing data privacy and cyber-security policies and companies' compliance with those policies; and representations about security breaches, Rawson said. At a minimum, representations function to put the seller on notice, bring attention to issues that may need addressing, and shift risks to the seller, where appropriate, he said.

In addition to reps and warranties, due diligence—as best as it can be done—also plays an important role. Violetta Kokolus, special counsel at Dechert who advises on complex technology and intellectual property transactions, recommends the following key measures.

- **Review the data that is collected and how it's used.** "If you don't understand what data is collected and how it is used, you will not be able to assess the legal risk," Kokolus said.
- **Assess data flows.** "Has it been exported out of the country? Has it been passed on to third-party vendors? All this information is relevant in terms of diligence," Kokolus said.
- **Pay attention to the location of third-party vendors.** Do you have cloud servers that are not based in the United States?
- **Review privacy promises of the target company.** "One of the most important things to do is to review that privacy promise: Can you purchase that data from the target and use it in the way that you want as a buyer? Look at privacy policies of affiliates, as well, to see if they are collecting different types of data. All of this is important to review," Kokolus said.

Not all target companies have a sophisticated understanding of data privacy and cyber-security issues. They may not even know if a data breach has occurred. Regardless of a target company's level of sophistication, "diligence plays a key role," Kokolus said.

The buyer company is not looking to educate the target company, but it can conduct its own investigation. One example is to engage the help of a third party, with the consent of the target, to conduct penetration testing.

Cyber-security considerations

The term "cyber-security" refers to an organization's systems as a whole—proprietary data,

business information, and personal information. Cyber-security also refers to the protection of personal information and personal data, a focal point for regulators.

It's important to ensure that the target company has a comprehensive information-security program in place. "Asking for privacy and information-security programs and getting from the potential target company its privacy policy is not sufficient," said Hilary Bonaccorsi, an associate with law firm Dechert.

Rather, when looking for cyber-risks in an M&A transaction, Bonaccorsi said some things to watch for include:

» **A written information security program (WISP).** The WISP should address how the company protects personal information, or employee information, that it collects and retains. It sets out the technical, administrative, and physical safeguards that the company has in place.
» **An incident response plan.** This is an action plan that generally explains what the company would do in the event of a data breach or a cyber-attack. "It lays out how a company determines whether a given incident constitutes a reportable event, how incidents will be escalated within the organization, and the names and contact information for given internal decision makers and stakeholders," Bonaccorsi said.
» **Contracts with critical third-party vendors.** Target companies often will say that they have customer data but, because they host it in the cloud or store it with a vendor, they don't have anything to show in terms of how they are protecting that data. "If it's your customers' information—even if you're hosting it on the cloud or with a third-party vendor—you are still responsible for it," Bonaccorsi said.
» **Contractual protection of personal data.** A purchasing company would want to see evidence from a target company taking this approach that it has conducted diligence itself in selecting a service provider or vendor, she said. One way to do that is to contractually require the vendor to protect personal data in the same way that the company would want it protected.
» **Evidence of cyber-liability insurance coverage.** It's not required for every company to have dedicated cyber-liability insurance. Such coverage, however, "becomes important in your diligence process as you're looking at potential data issues that a company may have," Bonaccorsi said. Something to keep in mind: not only if the company has cyber-coverage, but whether it feels it has enough cyber-coverage.

During an M&A transaction, it's also critical to ensure that data privacy and cyber-security policies are being implemented in practice. "A comprehensive information-security system and privacy policy can't just exist on paper," Bonaccorsi said. "Otherwise, they are essentially meaningless."

One way to go about determining whether a program is implemented is to request additional documentation—such as risk assessments that the company has performed on its IT systems, or penetration-testing reports. "Those could give you some idea about the level of engagement the firm has with cyber-security and what risks need to be dealt with or have been dealt with," Bonaccorsi said.

The organization could also request data incident reports. Documentation of claims made under a cyber-liability policy may also provide some insight into the extent to which the company has implemented data privacy and cyber-security policies and procedures.

Finally, you should determine whether there have been any data incidents or regulatory issues concerning the company and how those issues were resolved or if they're ongoing. These may include current or past information requests from regulators, for example.

In any merger and acquisition deal, conducting a robust level of due diligence is only half the battle. Putting in place representations and warranties in a purchase agreement, particularly as it concerns data privacy and cyber-security matters, is becoming an increasingly important measure in ensuring a smooth and risk-free transaction. ■

A look at China's sweeping new cyber-security law

Beijing has officially put foreign companies operating within China on notice: Improve your data privacy practices and cyber-security controls, or face the consequences. **Jaclyn Jaeger** reports.

The recent adoption of China's sweeping cyber-security law, and a follow-up draft security review framework published in February, serves as a stern warning to foreign companies in the country that it's time to reassess your data privacy practices and cyber-security controls.

The Standing Committee of the National People's Congress, China's top legislature, passed the "Cyber-security Law of the People's Republic of China" in November. It took effect June 1, 2017.

China's cyber-security law primarily applies to the "construction, operation, maintenance, and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China," according to an unofficial English translation of the law provided by China Law Translate. The overall intent, the law states, is "to ensure network security, to safeguard cyber-space sovereignty, national security, and the societal public interest."

One provision that has garnered a significant amount of attention from foreign companies in China is the data localization requirement. That provision requires that personal information and other

"important data" gathered and produced by "critical information infrastructure" (CII) operators must be stored on servers physically located within mainland China.

This could pose challenges for multinational companies needing to transfer data across borders in their business operations; foreign companies subject to the law would need to get government permission before transferring data out of the country. "The law is significant, as it is China's first to enact rules on the collection and use of personal data," states a report by the Information Technology & Innovation Foundation, a Washington think tank.

According to the law, "personal information" broadly refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, addresses, telephone numbers, and more.

CII operators found in violation of the data localization provision will be sanctioned with a warning, or worse, the confiscation of unlawful gains, Website shutdown, revocation of relevant operations permits, or a fine ranging between RMB 50,000 and 500,000. Individuals who are directly in charge will be fined between RBM 10,000 and 100,000.

Data protection measures. The cyber-security law also imposes numerous data protection measures on network operators, defined as "network owners, managers, and network service providers."

The data protection measures required by the law are the same measures many companies have already implemented as best practice, including:

» Strictly maintaining the confidentiality of user information they collect;
» Making data privacy notices publicly available, explicitly stating the purposes, means, and scope for collecting or using information;
» Adopting technical measures to ensure the security of personal information and prevent against loss, destruction, or leaks; and
» In the event of a data security breach, taking immediate remedial action and promptly notifying users and relevant authorities.

Furthermore, the law states that network operators shall not provide an individual's personal information to others without the individual's consent or illegally sell an individual's personal data; gather personal information unrelated to the services they provide; or disclose, tamper with, or destroy personal information that is gathered.

The various requirements concerning personal information are not that different from other regulatory regimes, such as the European Union's General Data Protection Regulation (GDPR). "The key difference is the need to obtain consent from the individuals concerned," says Clarice Yue, a senior managing associate at Bird & Bird in Hong Kong.

"In other words, China requires both notification and consent, and this is not restricted to direct marketing or transfer of sensitive personal information," Yue says. "A lot of the companies operating in China are already familiar with this dual requirement as they do appear in other key legislation, such as the PRC Protection of Consumer Rights Law." Various national standards on network security also exist, which will provide useful guidance to companies, she says.

Cyber-security reviews. Another provision raising concerns among foreign technology companies in China stipulates that network security products and services procured by CII operators that may impact national security must pass a cyber-security review.

Examples of key infrastructures cited by the Chinese government are expansive, sweeping in public communication and information services, energy, water resources, financial services, public service, and e-government affairs. In practical terms, any of these sectors could be required to use only computing equipment approved by state authorities to pass a security review.

The scope of those security reviews may be expanded even further, under a draft security review framework issued in February by the Cyberspace Administration of China (CAC), China's chief internet regulator. The draft measures appear to broaden the scope of cyber-security reviews by loosely stating that "important network products and services" used in information systems in connection with national security and the public interest are subject to its inspection requirements.

The Administration, together with other unidentified authorities, will form a newly established "network security inspection committee," tasked with administering inspection policies and overseeing network security inspections. According to the draft measure, cyber-security reviews primarily will focus on the "security and controllability" of the following risks:

» **Operation risks:** illegal control, interference, or interruption to the operation of these products and services;
» **Supply chain risks:** risks in research and development, delivery, and technical support activities;
» **Data-security risks:** the risk of providers using products and services to illegal collect, store, and process data; and
» **User-dependency risks:** risks associated with suppliers of network products and services drawing on user dependency to unfairly compete or impair their users' interests.

The focus on user-dependency risk is particularly concerning for foreign technology companies "whose products and services, even without monopoly behaviors, may dominate the market due to their competitiveness and the lack of alternative products and services," states a client alert from law firm Davis Wright Tremaine.

Neither the cyber-security law nor the draft measures spell out what information will be required for a cyber-security review. Without detailed guidelines, it is unclear to determine for hardware products, "what and how detailed technical documents should be provided for review," and for software products, "whether source code and decryption algorithm should be disclosed to the government," the Davis Wright client alert states.

According to the draft measure, a cyber-security review may be initiated at the request of a government agency, trade association, incidents in the market, or if a company voluntary submits its product or service for review. Once the cyber-security review is initiated, an authorized third party will evaluate the products and services first, followed by an overall assessment conducted by an expert panel.

The cyber-security review committee will then make a decision based on the expert panel's assessment report. With no appeal mechanism mentioned, it appears the committee's decision will be the final decision.

The review process itself will consist of four elements: lab testing, an on-site inspection, online monitoring, and review of background information. The draft measure is silent, however, on the overall timeframe of each element of the review or the review as a whole.

Network products and services that fail to pass a cyber-security review will be prohibited from being procured by party and government departments and operators of key industries. Companies seeking to supply network products and services to operators of CII in China—such as energy, finance, and telecommunication—should stay on top of these developments.

"As the draft measures come into force in the coming months, such companies will need to carefully assess the implications of the draft measures, including whether to voluntarily seek security reviews for their products or services," states a client alert from law firm Covington & Burling.

Data-security obligations. Most of the data protection-related requirements are not new. In fact, many of the cyber-security requirements can be found in sector- or industry-specific regulations.

"It is, however, the first time that we have a piece

"There is no subpoena process in China, Your data is really at the mercy of the Chinese government."

Dan Whitaker, Managing Director of China Operations, Consilio

of overarching legislation codifying all these requirements," says Michele Chan, a partner at Bird & Bird in Hong Kong. "The 'new' compliance requirements—which certainly are not new to telecom companies or financial institutions—relate mostly to cyber-security."

For example, companies are required to:

» Appoint a cyber-security officer;
» Implement measures to protect against viruses, cyber-attacks, and invasion;
» Record and monitor the relevant network and network incidents (retain network logs for at least six months);
» Adopt measures such as data classification, back-up of important data, and encryption; and
» Formulate emergency response plans for network security incidents, and periodically organize drills.

"Technical support" to enforcement authorities. Another provision in the law requires network operators to provide "technical support" to authorities for national security and law enforcement purposes. Some in the industry have concerns that this could include forcing companies to build backdoors to their encryption.

"There is no subpoena process in China," says Dan Whitaker, managing director of China operations at e-discovery and managed review provider Consilio. "Your data is really at the mercy of the Chinese government."

Whitaker, who serves as vice chair of the technology and innovation committee at the American Chamber of Commerce in Shanghai in a volunteer capacity, says China's anti-corruption law is currently a "big topic" of concern.

In fact, the American Chamber of Commerce in Shanghai is among more than 40 international business and technology groups representing hundreds of companies that expressed "deep concern" about several sweeping provisions in the law in a letter to the Chinese government.

Specifically, the groups' letter states, "We remain particularly concerned about provisions in the new cyber-security law and related measures that mandate broad data residency requirements and restrictions of cross-border data flows, trade-inhibiting security reviews and requirements for ICT products and services, and broad requirements for data sharing and technical assistance that may decrease the security of products and harm consumer privacy."

Given that numerous terms in the law remain vague and unclearly defined, potential CII operators in China should continue to proactively engage in discussions with industry groups and corporate counsel on how to best comply with the law.

"A preliminary self-assessment can be conducted to assess the risks for compliance," writes Xiaoyan Zhang, counsel at law firm Mayer Brown in Shanghai. "Tools such as data maps can be used to identify the physical locations of data and data flow charts to track the data's life cycle. Extra caution must be taken to ensure that legal requirements and technology jargon are not lost in translation during internal communications."

Further guidance, which companies should closely monitor, is expected to be published in the coming months. The law itself only sets out a framework. Forthcoming rules and standards are what will provide more concrete guidance to companies as to how best comply with the new law. ■

DRAFT MEASURES

Below is an excerpt from the draft measures on the security review of online products and services.

Article 6. The Cybersecurity Review Commission shall engage related experts to establish an expert panel which shall, based on third-party evaluation, conduct a comprehensive evaluation of the security risks of online products and services, and the security reliability of the providers of such products and services.

Article 7. Third-party cyber-security review agencies shall be exclusively identified by the government and shall perform third-party evaluation services in the cyber-security review.

Article 8. Based on the requirements of related government departments, suggestions of national trade associations, market feedback and corporate applications, etc., the Cybersecurity Review Office shall organize third-party agencies and experts to conduct cyber-security review of online products and services and publish or circulate to a certain extent the review results.

Article 9. The competent government departments of key sectors such as finance, telecommunications, and energy shall organize the implementation of the cyber-security review of online products and services in their respective industries or sectors pursuant to the requirements for the national cyber-security review.

Article 10. The Party and government departments as well as key industries shall give priority to online products and services that have passed the review in procurement, and shall not procure any online products or services that fail to pass the review.

Article 11. Where any online products or services that are purchased by critical information infrastructure operators may affect national security, such products or services shall be subject to the cyber-security review. Whether any online products or services purchased by critical information infrastructure operators affect national security shall be determined by the authority that is responsible for protecting critical information infrastructure.

Article 12. Third-party agencies performing the cyber-security review shall adhere to the principles of objectivity, fairness, and justness and carry out evaluation of online products and services and providers focusing on the controllability, transparency and creditability, and be responsible for the review results.

Article 13. Providers of online products and services shall cooperate in the cyber-security review. Third-party agencies and related organizations and personnel shall undertake the security and confidentiality obligations for any information learned in the review and shall not use such information for any purpose other than the cyber-security review.

Article 14. The Cyber-security Review Office will issue the security evaluation reports for providers of online products and services from time to time.

Article 15. The National Internet Information Office shall be responsible for the interpretation of these Measures.

Source: Chinese government (translation provided by Covington & Burling)

Identifying inside threats to cyber-security

To better manage and prevent insider-risk exposure, companies still have much to learn both from corporate data breaches of the past and from those that have developed best-in-class insider-threat programs. **Jaclyn Jaeger** has more.

Even as attacks on corporate networks become more prevalent, insider threats continue to pose the biggest data breach risk for companies in all industries and across all geographies. To better manage and prevent this risk exposure, corporate leaders still have much to learn both from corporate data breaches of the past and from those that have developed best-in-class insider-threat programs.

Findings from several recent surveys highlight the extent of the insider-threat landscape. Kroll's *Global Fraud and Risk Report*, for example, found that the biggest internal threats are current, former, or temporary employees.

In the Kroll report, 79 percent of 555 senior executives worldwide across multiple industries and geographies identified perpetrators as being:

» Internal senior or middle management employees;
» Internal junior employees;
» Former employees; or
» Temporary employees.

"Insider threats can take many forms, from unhappy employees with malicious intent to careless workers who inadvertently install malware, or even third parties that don't follow security policies," Kevin Jacobsen, executive director of EY's Fraud Investigation & Dispute Services (FIDS) practice, said during a Webcast on insider threats.

Ernst & Young's latest "Global Information Security Survey" further highlighted the type of insider-threat vulnerabilities that have most increased companies' risk exposure over the last year. The top vulnerabilities, cited by the 1,735 executives polled, are careless employees; unauthorized access; and outdated information security controls or architecture.

"Insider threats can take many forms, from unhappy employees with malicious intent to careless workers who inadvertently install malware, or even third parties that don't follow security policies."

Kevin Jacobsen, Executive Director, EY, Fraud Investigation & Dispute Services

In addition, the Kroll report cited similar vulnerabilities. Specifically, the highest reported attack vector, cited by 26 percent of respondents, occurred from a software vulnerability. The second and third most commonly cited causes for cyber-incidents were "employee error" and "attacks on the corporate Website," each cited by 22 percent of respondents.

The theft of physical assets was the most common type of fraud experienced over the past year, cited by 29 percent of respondents. The other top two most common types of fraud cited were vendor, supplier, or procurement fraud (26 percent) and information theft, loss, or attack (24 percent).

In a third survey, the Ponemon Institute's latest "Cost of a Data Breach Study" found that most data breaches were caused by hackers and criminal insiders, including employees, contractors, or other third parties. Among the 383 participating companies, 48 percent of reported breaches were caused by criminal or malicious attacks, such as malware infections and phishing schemes.

"It is hard to underestimate or understate the level of threat that companies are subject to from outside penetration in the form of hacking and phishing schemes," says Daniel Karson, chair of Kroll's Investigations and Disputes practice. "The bad guys only have to be right once." Companies most vulnerable to an attack are those whose information security systems are not state-of-the-art, or are not up to industry standards, he says.

In the Kroll report, the most frequent type of cyber-incident, cited by 33 percent, was a virus or worm infestation, whereas 26 percent of respondents cited e-mail-based phishing attacks as the second most frequent type of cyber-incident.

It is also important to note that malicious or criminal attacks vary significantly by country, according to the Ponemon Institute data breach study. For example, 60 percent of all breaches in the Arabian region (United Arab Emirates and Saudi Arabia) and 54 percent of all breaches in Canada were due to hackers and criminal insiders.

Among South African companies, only 37 percent of all data breaches were due to malicious attacks, with the highest percentage due to human error. Indian companies, in comparison, were most likely to experience a data breach caused by a system glitch or business process failure (37 percent and 35 percent, respectively).

Case study: Lockheed Martin

All of these insider-threat characteristics combined—the type of perpetrator, the form of attack, and the region of a data breach—should be taken

into consideration when implementing a state-of-the-art insider-threat program, given that each demands different response tactics.

During the EY Webcast, Doug Thomas, director of counter-intelligence at aerospace giant Lockheed Martin, shared the arduous journey that Lockheed took to implement its state-of-the-art insider-threat program. That journey started with getting buy-in from the senior leadership team, including the chief executive officer, chief operating officer, the executive vice president, and senior vice presidents—a process that was much easier said than done.

Developing an insider-threat program that was legally and regulatory sound was the easy part; what was difficult was aligning it with Lockheed's corporate values, Thomas explained. "Just because you can do something doesn't mean it's the right thing to do," he said. "You have to tailor your program to your culture."

Although Lockheed's senior leaders were more than willing to embrace counter-intelligence tools to spot and mitigate external threats to the company, some were not as comfortable with the idea of monitoring human behavior, which was the biggest sticking point.

Many employ technology that monitors only online anomalous activity or behavior, such as downloading sensitive company information at a higher volume than other employees, for example. "If you have a data loss prevention tool, and you think that's your insider-threat tool, you're mistaken," Thomas said. "That's only half the solution to the problem."

If you're truly going to have a robust insider-threat

PERPETRATORS OF FRAUD

Kroll's *Global Fraud and Risk Report* revealed that threats most commonly come from within. See below.

Nearly 8 out of 10 respondents (79%) cited one of the following categories as the key perpetrator:

- Senior or middle management employees of our own company
- Junior employees of our own company
- Ex-employees
- Freelance/temporary employees

Reflecting the complexity of fraud risks, the majority (60%) of executives who reported suffering fraud incidents identified some combination of perpetrators, including current employees, ex-employees, and third parties, with almost half (49%) involving all three groups. Nearly four in ten respondents (39%) who were victims experienced fraud at the hands of a junior employee, 30% at the hands of senior or middle management, 27% by ex-employees, and 27% by freelance/temporary employees. Agents and/or intermediaries, who are sometimes considered quasi-employees, were also cited by 27% of respondents as involved in carrying out fraud. While insiders are cited as the main perpetrators of fraud, they are also identified as the most likely to discover it. Almost half (44%) of respondents said that recent fraud had been discovered through a whistleblowing system and 39% said it had been detected through an internal audit.

Kroll experts Alex Volcic and Yaser Dajani write ... that it is important to triage whistleblower reports appropriately and test methods of escalation to run an effective system.

Source: Kroll

KEY STEPS FOR BUILDING AN INSIDER THREAT PROGRAM

1. Gain senior leadership endorsement, develop policies that have buy-in from key stakeholders, and take into account organizational culture;

2. Develop repeatable processes to achieve consistency in how insider threats are monitored and mitigated;

3. Use analytics to strengthen the program backbone, but remember implementing an analytical platform does not create an insider threat detection program in and of itself;

4. Coordinate with legal counsel early and often to address privacy, data protection, and cross-border data transfer concerns;

5. Screen employees and vendors regularly, especially personnel who hold high-risk positions or have access to critical assets;

6. Implement clearly defined consequence management processes so that all incidents are handled following consistent standards, involving the right stakeholders;

7. Create training curriculum to generate awareness about insider threats and their related risks;

8. Leverage information security and corporate security programs, coupled with information governance, to identify and understand critical assets.

Source: EY FIDS

program, Thomas said, you have to also understand the human behavior element. For Lockheed, the idea was to monitor every aspect of employee behavior.

To overcome any doubts, Lockheed created an insider-threat advisory review committee, made up of human resources, compliance, legal, privacy, ethics, and information security. This committee was tasked with writing a "Concept of Operations," describing what the insider-threat program is and is not, Thomas explained. "This is a team sport," he added. "Where you house this doesn't really matter."

"While we were building this Concept of Operations, I can't tell you the amount of conversations that went into privacy and the importance of the communication campaign," he said. Absolute transparency in the purpose and objective of the program is paramount.

"We don't profile people; we profile behavior," Thomas said. "We have a human behavior and digital behavior baseline of everybody in the company. You're looking for anomalous behavior."

For example, if somebody intentionally violates policies, especially IT policies, that could signal a red flag. Personal financial stressors or behaviors in the workplace, including the quality and quantity of the employee's work, are also signs of human behavior to keep any eye on.

"One person you need to get in front of is first-line supervisors, because they are the ones who are going to know their employees the best to see if there have been any changes or concerning behavior," Thomas said.

If a supervisor or other employee 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. To help foster a speak-up culture and encourage people to come forward, however, "we don't use the word 'report,' " Thomas said. "We're not encouraging our employees to 'report,' because we don't want to create a culture of snitches." Instead, he said, "we want employees to be 'engaged.' "

Also, Lockheed has in place a "very robust governance structure," Thomas explained. At the vice-president level is a steering committee that has to approve any changes or enhancements made to the Concept of Operations, and every three months the steering committee is briefed on the program.

Further, because espionage and information theft for the company is a high risk, Lockheed's risk and compliance committee is also briefed every six months. Internal audit is also invited every year to audit the program, and the board of directors is briefed every nine months on the program itself.

Another important aspect of establishing robust insider-threat programs and procedures is to have clear policies and procedures from the get-go. What does the company consider to be confidential and proprietary information? What are its crown jewels?

In those policies and procedures, "you want to reserve the right to monitor and inspect company systems and devices that you've provided to the employee," Luke Dembosky, a cyber-security partner at law firm Debevoise & Plimpton, said during the Webcast. If the company allows employees to use their own devices to access the corporate network, make sure you delineate exactly what inspection and monitoring rights the company maintains, he said.

Companies must also limit employee access to certain systems through network segmentation. "This is where your insider policies and procedures marry up with broader cyber-security defenses," Dembosky said.

Finally, training employees is also an important element of an insider-threat program not just to educate employees on how to spot insider threats, but also to remind them about the company's policies and procedures, Dembosky added. It's also important to log who showed up, so that if a legal matter were to arise, the company has that documented evidence to show that the employee was aware of the policies and aware of the company's inspection and monitoring rights, he said.

Looking ahead

In many respects, insider threats and outsider threats are one in the same. In fact, increasingly, malicious outsiders are using internal "spotters" to identify specific targets, server information, and individuals to be hacked—and, what is more troubling, is that these people can stay active in the organization for a long time without being discovered, Dembosky warned.

As organizations and government agencies fortify their networks, "you're going to see more human-enabled cyber-attacks—and that is your insider," said Louis Bladel, executive director of Ernst & Young and former special agent in charge of the Counterintelligence Division of the FBI's New York Field Office.

All of this is to say that companies must continue to do everything in their power to enhance their cyber-security defenses. With time, the risk will grow only more complex, and the repercussions, more severe, making a resilient insider-threat program more critical than ever before. ■

"If you have a data loss prevention tool, and you think that's your insider-threat tool, you're mistaken. That's only half the solution to the problem."

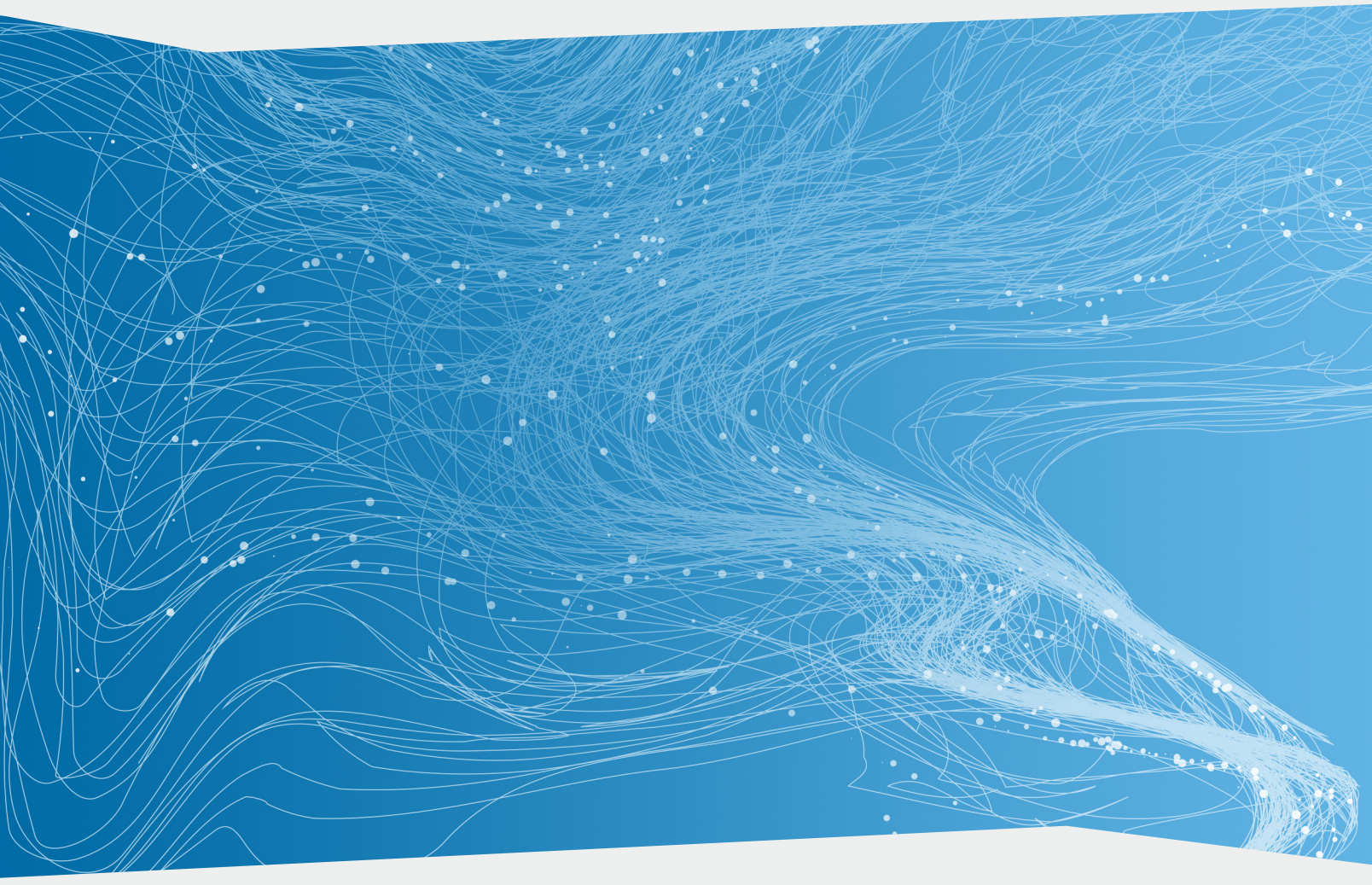
Doug Thomas, Director of Counter-Intelligence, Lockheed Martin

RSA

BUSINESS-DRIVEN SECURITY™ SOLUTIONS

The General Data Protection Regulation ("GDPR"), the European Union's new data protection law, represents a major evolution in global data security and privacy practices.
Visit www.rsa.com/gdpr to learn how RSA Business-Driven Security solutions can help your organization address GDPR compliance obligations.

RSA



WHITE PAPER

GDPR: WHAT IT MEANS TO YOUR CYBERSECURITY STRATEGY

RSA

INTRODUCTION

Modern IT, especially cloud and mobile technologies, has significantly improved access for users from anywhere to anywhere. Whether a user is working remotely and needs to access company systems; taking advantage of 24hr banking to manage their finances; or buying online to avoid shopping crowds; people have amassed a multitude of online "identities" in their effort to improve efficiencies of many day-to-day tasks. Users are not just employing one device, in fact, they typically intermingle an assortment of corporate-issued and personal devices.

Essentially, Modern IT is designed to create cost efficiency and convenience around communications and transactions. The complication is that these benefits are not limited to the organizations and their authorized users but extend out to hackers/cyber criminals. The plethora and intermingling of both personal and company-issued devices added to the swelling number of cloud applications has massively enlarged the attack surface increasing the complexity of protecting an organization while at the same time decreasing the difficulty for compromise.

While organizations try to create friction for unauthorized users by adopting best-in-class technology and hiring skilled cybersecurity professionals, the European Union (EU) has announced a regulation that is "designed to harmonize data privacy laws across Europe, protect and empower all EU citizens data privacy, and to reshape the way organizations across the region approach data privacy." While the EU has had data privacy laws since the 1980's, this is the first regulation that applies directly to organizations established outside the EU that process EU citizen personal data. The GDPR will be a game-changing regulation because it is basically resetting the best practices model for data privacy and protection, globally as the first pan-EU law that is also extraterritorial.

WHAT IS THE GENERAL DATA PROTECTION REGULATION (ALSO KNOWN AS THE "GDPR")?

The General Data Protection Regulation is a new piece of legislation that is scheduled to become effective in May 2018. This single Europe-wide regulation removes the complexities that organizations currently face around complying with multiple local data protection rules across the EU. Prior to GDPR, each of the 28 member states were permitted to interpret the existing rules in their own way, making compliance across the region complex and expensive.

The GDPR unifies EU data protection legislation. That, in turn, unifies processes and legal obligations for any organization doing business with more than one EU state.

RSA

The scope of the GDPR, however, substantially increases the obligations on organizations that are processors of EU citizen personal data. The penalties for non-compliance are substantial, which will propel data protection as a business risk directly into the boardroom.

WHY IS IT NECESSARY?

New technologies and globalization have transformed how organizations collect, access, and use information, including personal data. However, until the formation of the GDPR there were no consistent rules for managing personal data. In fact, even the 1995 Data Protection Directive, which was adopted by the member states of the EU, had inconsistent interpretations, resulting in divergent enforcement practices.

More than 90 percent of Europeans say they want the same data protection rights regardless of where their data is processed. So in January 2012, the European Commission in Brussels proposed a reform of the EU's 1995 data protection rules to "make Europe fit for the digital age." As such, the Commission pursued a *regulation* (one law that applies equally) rather than a *directive* (a law that member states can interpret individually). With this new regulation, the EU believes that they can eliminate fragmentation and create what has been termed a "one-stop shop" for data protection in Europe.

On 15 Dec. 2015, the European Parliament, the European Council, and the European Commission reached an agreement on a joint proposal for the new data protection regulation to establish a modern and harmonized data protection framework across the EU.

WHAT DOES THE GDPR EXPECT TO ACCOMPLISH?

The fundamental aim of the reform is to better protect the rights of individuals regarding their personal data. The GDPR defines personal data as "any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address." These rights span our lives at home, at work, as consumers, as patients, in legal matters, and on the Internet.

The GDPR also contains provisions specific to children. The main purpose of this provision is on commercial internet services such as social networking. If your organization collects children's personal data, you will need to have a system to verify children's ages; and have a process to obtain the consent of a child's parent or legal guardian.

While the GDPR is an essential step to strengthen EU citizens' fundamental rights in the digital age; it can also facilitate business by simplifying rules for organizations in the Digital Single Market. A single data privacy law will

RSA

eliminate the current fragmentation and costly administrative burdens, leading to savings estimates of around €2.3 billion a year.

In the law enforcement and criminal justice sectors, the GDPR is designed to safeguard citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. In particular, it will ensure that the personal data of victims, witnesses, and suspects of crimes are duly protected; and it will help cross-border cooperation in the fight against crime and terrorism.

TO WHOM DOES IT APPLY?

The GDPR applies to the collection of personal data of EU citizens *anywhere in the world*. Note, that GDPR compliance applies even if the data processor or data controller is outside the EU; they fall under the scope of the GDPR simply by processing EU citizen data. This includes organizations that provide cloud services to EU customers that are based outside the EU.

Because any organization that works with personal information relating to EU citizens will have to comply with the requirements, GDPR will become the first global data protection law. So the big question is, "how does this affect your cybersecurity strategy."

CYBERSECURITY AS BUSINESS DRIVEN SECURITY

The GDPR requires organizations to know exactly what, when, and where they are collecting information from covered persons, processing the information, storing the information (and how long), and sending information to others, including across borders. Moreover, all of this has to be sufficiently documented, the risks assessed, and appropriate technical and organizational measures implemented to bring residual risk within tolerable levels. Because of the required level of detailed documentation, it is unlikely that an organization can fulfill their obligations under the GDPR and demonstrate their compliance using spreadsheets and word processing documents. Compliance has to be independently verified so adequate and complete documentation will be critical to keeping audit costs down and audit and regulatory engagements and findings as short as possible.

In the process of an organization assessing their GDPR-related risk and determining the appropriate technical and organizational measure to treat the risk, organizations must understand the risk in business terms. Without translating technical risk into terms that senior business leaders can understand, it is difficult for the organization to make well-informed decisions about the allocation of scarce human and capital resources across the organization's risk portfolio. The application of a Business-Driven Security Strategy to GDPR will avoid this problem and promote better risk management practices of technical risk managers as well as business leaders.

RSA

WHAT DOES GDPR MEAN FOR YOUR GRC/BUSINESS RISK MANAGEMENT STRATEGY?

Business Risk Management / GRC tools play a critical role in helping organizations fulfill GDPR obligations.

- All GDPR-related infrastructure, business processes, policies and procedures, risks, controls, third parties, business resiliency plans, and outstanding issues and remediation plans must be documented.
- The level of GDPR-related risk must be assessed for every IT infrastructure element, business process, and third party where covered information is processed, stored, or transmitted. In assessing risk, consideration should be given to both electronic and physical security as well as to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to covered data.
- Documenting the implementation of appropriate technical and organizational measures to help ensure a level of security appropriate to the risk. Appropriate technical and organizational measures are to be designed to protect covered data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access or alteration of personal data.

Technical measures include technologies implemented to help protect and mediate physical and electronic access to your systems and data, detection tools to expose and respond to unauthorized access, etc. Organizational measures include policies and procedures around vetting new hires and third parties that handle or access covered data, data input and edit controls, data input and output file reconciliations, employee education and training around privacy, SDLC procedures incorporating information security assessments, third-party governance, business resiliency and the like.

- Documenting the results of periodic tests of technical and organizational measures to ensure that they continue to be designed and operating effectively. Testing may be performed manually or result from the implementation of automated continuous control monitoring.
- Monitoring the overall status of the GDPR risk profile. For most organizations, GDPR risk will not remain static. As the volume of covered data changes, the organization's products and processes change, and geographic footprint and third party dependencies change, so too will the organization's GDPR risk profile. As risk assessments and control testing are completed gaps in technical and organizational measures will be identified that must be remediated to comply with GDPR. By consolidating all of your GDPR-related compliance information in one platform, not only are you able to readily demonstrate compliance with GDPR but you are informed as risk increases, changes in the organization occur that warrant

RSA

attention, issues are exposed that must be actively monitored to remediated, and security incidents arise that must be actively managed and reported to authorities and the customers that may have be subject to the incident.

Above are the core elements necessary to transform a technical security approach to GDPR to one that is business driven. In addition, the following obligations imposed by GDPR can be documented with a configurable business risk management / GRC tool:

- Cataloguing and managing EU citizen inquiries about whether their data is being handled by the organization
- Steps taken to respond to EU citizen requests to be "forgotten"
- Managing exceptions to the explicit consent requirements of GDPR, including exceptions around the requirement to obtain parental consent for children under 16 years of age.

WHAT DOES GDPR MEAN FOR YOUR IDENTITY STRATEGY?

RSA believes that Identity is the most consequential threat vector with 63% of confirmed breaches in 2015 resulting from compromised credentials 81% of hacking-related breaches leveraged either stolen and/or weak passwords (2017 Verizon Data Breach Investigations Report). This underscores the need for stronger authentication mechanisms that are convenient to the end user, while still secure and in compliance with corporate and regulatory policies. Building a strong Identity and Access Management (IAM) program is central to reducing identity risks that can be exploited by hackers to infiltrate and steal personal information.

An IAM solution can help solve three fundamental challenges for organizations to protect sensitive and personal information: are my users who they claim they are; do they have the right level of access; and is the access in compliance with policies? First, organizations need to provide convenient yet secure access in order for users to find the information they need (regardless of whether the application is on premise or in the cloud) and deliver the confidence that people are who they say they are. Secondly, organizations need to ensure users have the appropriate level of access to do their jobs. This involves requesting, reviewing, granting, and revoking user access; using automated processes that enable business owners to make access decisions. Lastly, proving compliance is critical to showing regulators how organizations are complying with GDPR. With identity governance controls and reporting that connect back to corporate GRC policies, it is much easier and efficient to run reports to show continuous compliance aligned to the regulations. All three components provide visibility and control so that your organization can maintain continuous compliance.

RSA

Compromised accounts, stolen credentials, or mismanaged provisioning all could be seen as a weakness in GDPR compliance. Organizations need to show they are taking a proactive approach to managing access to personal information. In the event of a breach, comprehensive audits to prove a high level of access control will help strengthen the argument that the organization made a conscientious effort in line with GDPR guidance to protect identities. As we know, the costs of non-compliance with GDPR are steep, up to 4% of annual global revenue or €20 Million (whichever is greater). Therefore securing your identities and access governance are imperative steps to help meet GDPR requirements.

WHAT DOES THIS MEAN FOR YOUR THREAT DETECTION & RESPONSE STRATEGY?

Many organizations have deployed technical measures around data protection infrastructure, ranging from firewalls and spam filters, to Data Loss Prevention (DLP) solutions and Intrusion Prevention Systems (IPSs). Still, we hear about data breaches that affect millions of users.

Breaches continue because, as security infrastructure became standardized, threat actors have become adept at targeting attacks and evading defenses. The operating presumption must be that your organization's IT infrastructure is under continuous attack, and potentially already compromised in multiple ways. This shifts the conversation from threat prevention, to threat detection and response.

Organizations should consider technology solutions that provide visibility across the network utilizing data from logs, packets, endpoints, and threat intelligence to rapidly detect and understand the full scope of a compromise to aid in fast and effective response.

By using solutions with behavioral analysis and machine learning, organizations can correlate indicators and assigns risk scores that identify anomalies that warrant investigation. Unlike traditional prevention systems, this will help your organization hunt for the threats that have successfully invaded your organization. Undetected, such exploits can wreak havoc on your infrastructure and intellectual property, and can lead to the types of data breaches of EU citizen personal data that the GDPR specifically covers.

Another consideration, would be to adopt a solution that allows for configuration to limit exposure of privacy-sensitive metadata and raw content (packets and logs) using a combination of techniques, including:

- Data Obfuscation – Privacy-sensitive metakeys can be obfuscated for specified analysts/roles
- Data Retention Enforcement – Retain privacy-sensitive data only as long as needed

RSA

- Audit Logging – Audit trail for privacy-sensitive activities, e.g., attempts to view/modify data

SUMMARY

Ultimately, the objective of the GDPR is to shield all EU citizens from privacy and data breaches in an increasingly connected and data-driven world. GDPR modernizes and expands the 1995 Data Protection Directive to drive uniformity around interpretation and implementation of data protection rules as well as territorial reach to include any organization, in any country that is a controller or processor of EU citizen personal data.

EU citizens are entitled to key personal data protection "rights' under GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure – also known as the right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object

A tiered approach to fines has been established by GDPR stretching from 2% of annual global revenue for not having their records in order, not informing the supervising authority and data subject (individual) about a breach or not conducting an impact assessment to up to 4% of annual global revenue or €20 Million (whichever is greater) for the most serious violations; e.g. not having sufficient customer consent to process data or violating core concepts. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement. In other words, failure to comply could be debilitating for some organizations.

BUSINESS-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA is a leader in advanced cybersecurity solutions delivering Business-Driven SecurityTM so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid response and detection, control at the user access level, and business risk management.

The **RSA® Archer® Suite** is engineered to empower organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

The **RSA® SecurID® Suite** is designed to enable organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness designed to ensure the right individuals have the right access, from anywhere and any device.

The **RSA® NetWitness® Suite** is a threat detection and response platform that is designed to allow security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Suite is engineered to provide the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

ABOUT RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.