Bloomberg BNA

Privacy and Security Law Report®

A Guide for Insurers on Creating and Maintaining a Cybersecurity Plan

BY ELIZABETH TOSARIS

The intersection of valuable and personally identifiable digitized information and the increasing incidence of cybersecurity breaches makes the creation and maintenance of a cybersecurity plan one of the most pressing concerns for every insurer doing business in the U.S. This article lays out a basic framework for a cybersecurity plan, an insurer, particularly an insurer holding health data, can use when designing and updating its cybersecurity program.

The news has been full of reports of cyberattacks on American businesses and the resulting breaches of companies'—and their customers'—most sensitive data. Insurers, particularly health insurers, are not immune to these attacks; criminal attacks in health care are up 125 percent since 2010, and are now the leading cause of data breaches.[1] However, health insurers are not the only insurers that maintain the kind of medical and personal information that has been the targeted: Carriers writing accidental death and dismemberment, disability and long-term care insurance also have reason to gather and retain sensitive medical information, which could make them targets. Auto insurers and other liability writers may gather detailed personal information about both insureds and claimants who have suffered bodily injury. So it is not terribly surprising that in June 2015, the North Dakota state workers compensation carrier announced that its server suffered a breach that may have led to the disclosure of consumer information.[2] And other insurers also maintain information other than health data that could be a tempting crime target. For example, financial guaranty companies have detailed financial information on their insureds, while surety companies may also obtain detailed financial pictures of individuals as well as businesses.

The type of personal information maintained by insurers may include individuals' names, Social Security numbers, Medicare numbers and health condition and treatment histories. Because there is so much information aggregated in one place on each individual, there is the potential for a higher return when that information is stolen and sold. In addition to the usual crimes of identity theft, health data can also be used to commit the costly crime of medical identity theft, which occurs when stolen personal information is used to obtain medical care, purchase drugs, submit fake billings to Medicare or purchase medical equipment for resale. Unlike financial information, which can often be voided in favor of new information, such as a new credit card number or a new bank card PIN, health data often cannot be changed to protect the individual from a breach. So it is hardly surprising that personal information relating to health is targeted by cybercriminals seeking to monetize the data in black markets. Consequently, medical files, as well as billing and insurance records, are the top stolen targets.[3] Insurers as well as hospitals have recently experienced breaches. And in both cases, since the theft of health data is often not discovered as quickly as financial fraud, the damage that can be caused by these thefts is considerable. For example, the breach can have a lasting effect if it leads to a person's medical history containing false information.

Of course, simple theft may not be the only reason for a cyberattack. Other possible reasons include targeting

[1] Ponemon Institute LLC, *Fifth Annual Benchmark Study on Privacy and Security of Health Data* (May 2015) (14 PVLR 841, 5/11/15).

Elizabeth Tosaris, a partner in the San Francisco office of Locke Lord LLP, has nearly 25 years of insurance regulatory and insurance litigation experience. She assists clients on a broad range of issues arising out of the regulation of the insurance industry, such as cybersecurity, sophisticated market conduct and examination representations. She may be reached at (415) 318-8817 or etosaris@lockelord.com.

[2] Press Release, North Dakota Workforce Safety & Insurance, Cyber-Attack on State Server May Impact WSI Information, https://www.workforcesafety.com/news/news-item/cyber-attack-on-state-server-may-impact-wsi-information.

[3] Ponemon Institute LLC, *supra* note 1.

 ISSN 1538-3423

one company as a way to advance a different attack against another company, vandalism and malicious attacks as means of damaging the victim's reputation or ability to operate. Regardless of the reason for the attack, the cost to consumers and companies when these breaches occur is significant. Moreover, the larger the breach and the more malicious the attack, the higher the cost to the company, not just in absolute numbers, but also by a metric of dollars per lost or stolen record. The criminal intent, the consumer harm, the significant potential disruption to businesses and the magnitude of the cost means that the issue has received attention from government regulatory agencies (like the Securities and Exchange Commission) and attorneys general, the plaintiff's bar and even Congress and President Barack Obama.

Most companies focus on likely disaster scenarios in crafting their business continuity plans, with precautions for times when a data center is rendered inoperable by a natural disaster, and the backup plan is to move the functionality to another site until the problem is cleared. But planning for all or most of the insurer's computers to be rendered inoperable by a massive cyberattack should now be part of any organization's business continuity effort. Insurers that have not already should immediately begin creating a comprehensive security plan.

Insurers can do much both to secure their systems and to satisfy regulators, shareholders, consumers and others that they have taken reasonable steps to safeguard their confidential data. Having a prudent plan in place might also make the difference when establishing coverage under a cyber-insurance policy: In a pending coverage action involving an insured hospital system, the pleadings allege that the hospital system failed to ''continuously implement the procedures and risk controls identified'' in its insurance application, and that the data breach was caused by the system's:

> failure to regularly check and maintain security patches on its system, its failure to regularly reassess its information security exposure and enhance risk controls, its failure to have a system in place to detect unauthorized access or attempts to access sensitive formation stored on its servers and its failure to control and track all changes to its network to ensure it remains secure among other things.[4]

In addition, the strength and scope of a company's cybersecurity plan is now an important part of the due diligence review that precedes mergers and acquisitions transactions.

A successful plan should have the following four hallmarks:

Before, During and After Components: The company should not assume that its security is impregnable, and therefore should have contingencies established for the possibility of a breach. In addition, the company should assume that even after the breach itself has been addressed, additional action will be required of it in the aftermath of the breach.

Buy-In at All Levels of Company: Cybersecurity implicates many critical insurer functions as well as being integrally involved in sound corporate governance. Due to the high profile of the issue, regulators, shareholders and affected consumers expect the subject to receive attention from the highest levels of the company. Active monitoring by and direction from the board and/or chief executive officer are now common. And to the extent that expensive or resource-intensive initiatives are required to implement the plan, management involvement and support are imperative.

The Plan Must Be Thoughtful and Documented: Given the complexity of the issue, the plan should be the result of considered analysis from all the potentially affected areas. In addition, that work should be documented in a way that allows the company to memorialize the plan and also prove that it has taken reasonable and proactive steps both to minimize the risk of breach. Of course, a detailed and well-documented plan also aids the company in the event of any breach that might occur despite these efforts.

The Plan Must Be Flexible and Dynamic, Not Static: The plan should be flexible to allow rapid response to events and developments in the cybersecurity world. Not only is the technology that drives both the security and the ability of hackers to penetrate that security constantly evolving, but the rules and expectations for insurers using that technology is also in a state of rapid flux. A plan that is state of the art today may be hopelessly outdated less than a year later. Part of every plan must include the ability to reassess and update in response to new technology, new information and new standards. And there may be other resources that come online over time and should also be used. For example, the industry is already taking steps to coordinate how it responds to cyber breach incidents through groups designed to share information about digital threats—like the National Health Information Sharing and Analysis Center, or NH-ISAC.[5] In addition, the Department of Homeland Security has been in discussions with industry about the possible sharing of its hack attack database with the private sector.

In order to meet these four objectives, the remainder of this article discusses some more detailed guidelines for cybersecurity plans.

The Plan Must Comply With Applicable Privacy/Security Laws.

To date, no overarching legal framework has been established to address cyberattacks, although there already is a bewildering array of existing laws and regulations, new guidelines and general expectations that companies must understand and synthesize into their cybersecurity program. And these laws and their interpretations are far from static: For example, any further action in one of the several ongoing attorney general or department of insurance investigations of a health insurer breach, or the formal resolution of those investigations, will likely lead to further insight regarding standards of care for an insurance company.

Before any breach, legal counsel for the insurer should have a good understanding of the legal issues

[4] Judy Greenwald, *Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement*, Bus. Ins., May 15, 2015.

[5] The NH-ISAC organization teams private and public resources to provide members access to a secure information exchange infrastructure, including: best practices, standards and regulatory compliance guidance; risk management; and other relevant topics.

  PVLR ISSN 1538-3423

raised by a cyber incident. This includes familiarity with existing laws defining what information is private or confidential, and what types of security requirements apply to the various types of information. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, set forth rules that apply to health insurers and others who have access to protected health information.[6] And in the event of a breach of the protected health information, companies must follow Department of Health and Human Services requirements for reporting and notification. In addition, 20 states have a version of the National Association of Insurance Commissioners (NAIC) Model Insurance Information and Privacy Protection Act (Model 670), and these laws and regulations also impose requirements around the safeguarding of personal information.[7]

In the event of a cyber breach, insurers must identify the jurisdiction(s) where the breach occurred in order to know what laws apply. Next, the company must determine whether an actionable breach has occurred under the applicable state law definition. Definitions of breach vary widely, ranging from a requirement to perform a risk of harm analysis to a ''breach of security'' regardless of whether data are taken.[8] Only once the company has identified whether an actionable breach occurred can it determine what notification duties have been triggered. Different states have different rules on what constitutes a compliant notification, covering such topics as the method of transmission of the notice, the time in which notice must be sent and the information the notice must contain. Some states require notice to their department of insurance or attorney general as well as consumers affected or potentially affected. And information requested in state department of insurance notices can also go beyond reporting the simple fact of breach; they may also requiring reporting on tangential items, such Connecticut's requirements for a report on the results of any internal review identifying either a lapse in internal procedures or a confirmation that all procedures were followed.[9]

Information on what is required in the event of a breach must also be kept current: In response to recent events, several states have already made significant changes to their data breach notification laws this year.[10] In addition, companies will need to consider whether other remedial action is required: Later this year, Connecticut law will require a year of identity theft protection services for data breach victims.[11] California and Florida also have rules that address services related to a breach.[12] In general, regulators are concerned with the question of the financial impact of the breach on consumers, providers (in the case of health insurers) and, of course, the insurer.

In April 2015, the Cybersecurity Task Force of the NAIC adopted a list of 12 guiding principles that identify types of safeguards regulators expect insurers to have in place to protect consumers from cybersecurity breaches.[13] The principles direct insurers, producers and other regulated entities to join forces in identifying risks and adopting practical solutions to protect information entrusted to them. While these NAIC guidelines are aspirational and fairly nonspecific, they do provide useful policy directives that should be taken into account by insurers when formulating their cybersecurity programs.

In addition, multiple state departments of insurance, federal agencies and Congress have all begun further investigation into carrier's cyber vulnerabilities and the impact of breaches. Additional laws and guidelines should be expected as a result of the findings in those investigations. In April 2015, state insurance regulators and federal officials held meetings regarding best practices for cybersecurity in the insurance sector. The federal Department of Justice issued its own guidance, titled ''Best Practices for Victim Response and Reporting of Cyber Incidents,'' which outlines steps companies should take before, during and after an incident and provides a useful a checklist for companies.[14]

The Plan Should Clearly Identify the Insurer's 'Crown Jewels.'

The ''crown jewels'' are the data and systems that are most important to the insurer and its operations. By prioritizing these data and systems, the company knows where to direct maximum resources both before a breach and in the event of an actual breach. And, the insurer should be cognizant of the fact that as its systems are refined, either in connection with its cybersecurity efforts or as a result of normal business updates, exactly what constitutes these ''crown jewels'' may also evolve.

The Insurer Should Assess Its Risk on a Regular Basis.

Insurers should engage in periodic self-assessment efforts using a multidisciplinary team to help evaluate their risk. A risk assessment should identify those assets and systems where personal health information and other protected data reside. This information is needed not only to keep an insurer's plan current, but also in order to obtain the information necessary to

[6] HIPAA, Public Law 104-191; HITECH Act, Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

[7] These states are Arizona, Arkansas, California, Connecticut, Georgia, Hawaii, Illinois, Kansas, Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, Virginia, Wisconsin and Wyoming. *See, e.g.*, Cal. Ins. Code § 791 et seq.

[8] Not all states define a breach of security (*see, e.g.*, Wisconsin). In the majority of states, the law revolves around the question of whether it is reasonable to conclude that some sort of harm or unauthorized use has occurred. In contrast, in Connecticut and New Jersey, ''unauthorized access'' alone can be a breach if the data accessed included any of the statutorily defined targets.

[9] Conn. Ins. Dep't, *Bulletin IC-25* (Aug. 18, 2010).

[10] *See, e.g.*, Nev. A.B. 179; Conn. Substitute S.B. 949 (14 PVLR 947, 5/25/15; 14 PVLR 1244, 7/6/15).

[11] Conn. Substitute S.B. 949.

[12] Cal. Civ. Code § 1798.82; Fla. Stat. § 501.171.

[13] NAIC, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (Apr. 17, 2015), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[14] DOJ Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents* (Apr. 2015), *available at* http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf (14 PVLR 802, 5/4/15).

make any required reporting on enterprise risk. For example, Form F reporting requirements under the Holding Company Act generally ask for information on any event or circumstances involving the insurer or its affiliates that ''if not remedied promptly, is likely to have a material adverse effect upon the financial condition or liquidity of the insurer . . . .''[15]

The Plan Should Require Strong IT System Security.

An important and obvious step in maintaining security around sensitive data is to invest in a sophisticated security system and then continue investing the time and effort to keep the system as secure as possible. The system should provide for security around any social media used by the company, as it is estimated that as many as one-third of U.S. data breaches originate via social networks.[16] Security could include off-site data backup, intrusion detection capabilities and devices for traffic filtering or scrubbing. Having appropriate technology and services in place before an intrusion occurs is the first and best defense. The technical knowledge and technology required to accomplish these steps are beyond the scope of this article.

And of course the technology must also diligently monitor any attempts to breach or attack the system. Major insurers are subjected to a barrage of attacks on a daily basis. The majority of these attacks are not successful and are turned away at various points in the company's data security defense. But critical to the success of any cyber plan is the ability to know if there has in fact been a successful attack on the company, and to know this as soon as possible. This is particularly true in the case of attacks that are designed to penetrate the system and then remain in place in order to siphon out information on an ongoing basis. While in some cases an outside party, such as the Federal Bureau of Investigation, may be the one to notify the company of a breach, the more desirable circumstance is one where the company itself detects the breach soon after it has occurred.

Companies can test the strength of their systems using white hat penetration experts, which are in-house or third-party consultants hired to attempt to hack into the system as a means of identifying its strengths and weaknesses. Companies can also engage in security social engineering, which guards against employees accidentally creating vulnerabilities in the system. Common weaknesses include allowing employees to click on a link in an e-mail or website that is not secure, allowing employees to check personal e-mail on corporate computers or send e-mails and other outbound traffic overseas. (Security consultants generally counsel it is better to block all international access and then add exceptions for business purposes.)

There are also a number of rules that can be developed for maintaining security around routine access points. Common examples are implementing regular updates to token rings and having a minimum two-step encryption process. In fact, some states have a safe harbor for encrypted information. Other tools include employing a two-factor authentication process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code or even biometrics (e.g., fingerprints, iris scans, facial or voice recognition) for access. Companies also should not forget the importance of simple physical security, such as the screening visitors and locking access to sensitive areas. Insurers should have clear rules around employees' ability to use their own electronic devices in connection with company business (''bring your own device'' or BYOD rules).

The Plan Should Consider Best Practices for Training of Personnel.

Company personnel can be trained to avoid or minimize the risk of breach. All personnel should also be trained on physical security and maintaining a general attitude of vigilance. Another important component of this training involves strategies to identify and avoid phishing, as consultants report that a significant percentage of employees have been deceived by these counterfeit e-mails, and in some cases the result has been a breach. Depending upon individual job duties, company systems and platforms and the nature of the data held by the company, additional, more technical training may also be indicated.

Another effective training tool is staging a ''hack day'' in which the company practices the plan it intends to follow in the event of an actual breach. This is a time-honored method for preparation for other kinds of disasters and adapts easily to the cybersecurity arena. Having a dry run allows the company to identify and address potential glitches, oversights or other weaknesses in the plan and then correct them in order to further strengthen its defenses.

The Plan Should Consider the Purchase of Cyber Insurance.

Coverage for electronic breaches may be available under a variety of existing insurance products, and state and federal agencies are encouraging the insurance industry to offer even more and better coverage to U.S. businesses as quickly as possible. Specialty cyber liability policies typically cover reimbursement of expenses and costs of investigation with respect to the cause of a data breach; the cost of engaging a public relations firm; the recovery and/or recreation of the electronic data; the losses resulting from business interruption as a result of the breach; and the costs of the defense, loss, damages and expenses related to third-party claims arising out of invasion of privacy or any theft of personal and confidential data.

As part of its security plan, insurers should consider whether to purchase a cyber insurance policy, and, if so, what product is best suited to its needs. Part of this process includes analyzing the level of protection under existing commercial general liability coverage, crime and fidelity policies and specialty cyber liability policies. And since there is an effort on the part of regulators to expedite the development of new products, insurers should be sure to monitor the types of products available in the market on a regular basis to determine whether a more suitable product might be purchased as a substitute or supplement for existing coverage.

---

[15] NAIC Insurance Holding Company System Regulatory Act (Model 440) s. 1, subs. H.

[16] *See e.g.*, ZeroFOX, *The Anatomy of an Enterprise Social Cyber Attack [Infographic]*, https://www.zerofox.com/whatthefoxsays/the-anatomy-enterprise-social-cyber-attack-infographic/ (last visited Aug. 17, 2015).

  PVLR ISSN 1538-3423

The Plan Should Consider the Security of the Company's Vendors.

A chain is only as strong as its weakest link, and since many insurers rely upon vendors to help them run their operations, vendor security is an extremely important component of the overall security plan. More than one high profile breach in the last few years has occurred because of a breach in a vendor's system that allowed the hackers to enter the real target. For insurers, one of the most common categories of vendors is the insurance producer or agent. These producers may be captive agents or may be independent agents, but all of them are expected to gather sensitive information on behalf of the insurer. When these vendors' security is lax, it is a risk that translates directly to risk to the insurer.

Insurers can guard against this kind of breach by putting a number of safeguards in place when it comes to vendor relations. For new vendors, companies should conduct a cybersecurity due diligence before that vendor can ''enter'' the company's electronic environment. Where applicable, vendor contracts should contain rules regarding where vendors can store their data (in the cloud? offshore?), contain warranties and guarantees around security and possibly even require the vendor to carry its own cyber insurance policy. Finally, where relevant, the company should be familiar with vendor's disaster recovery plan and should compare that plan against company's own standards. Particularly where the vendor has access to sensitive and confidential data, the company should consider contractually imposing security standards on the vendor.

For existing vendors, the process can be a little trickier if it involves the renegotiation or amendment of existing contracts. Nevertheless, the company should assess the vendor's internal security as thoroughly as possible. Methods of assessment include conducting quality audits, which may include on-site assessments, asking vendors to complete questionnaires, imposing mandatory compliance standards and requiring vendors to obtain security certifications from recognized institutions. A number of large health-care insurers are requiring their business associates to conduct comprehensive assessments of the vendors' information technology privacy and security status and to obtain a certification of completion within a set time frame.

The Plan Should Lay Out a Course of Action in the Event of a Breach.

Insurers should also ensure that they have the technology and services necessary to respond to a cyber incident. For obvious reasons, the first priority after a breach is to understand the scope of the breach as soon as possible. The company will want to understand how the hackers got in, which computers and accounts were compromised, what data was accessed or stolen and whether any other parties—such as customers or business partners—were affected. This information is the foundation for repairing the breach and understanding what sorts of notifications are required as a result of the breach.

The security plan should include a list of people who should be alerted as soon as the breach is discovered, along with appropriate contact information. These individuals should include not just security experts, but legal counsel, individuals responsible for sending notifications and any others whose ability to execute core insurer functions will be impacted. The plan should not assume that it will be possible to send e-mails through the company's own system—when Sony Pictures Entertainment Inc. was hacked in 2014, its chief executive officer reported that senior executives had to develop a communications network using a phone tree where updates on the hack were relayed from one person to another via cellphones. And because computers were down, Sony staff ended up using cellphones, Gmail accounts and notepads to keep operations going. In addition, the company will want to involve relevant law enforcement and intelligence agencies. This may include the FBI, or the cybercrime unit of local or national law enforcement, as these agencies can help direct the company's responses to the breach.

As the repairs are put into place, it is important to keep the following three objectives in sight. First, the company will need to preserve evidence of how the hack was executed and how it responded. This will be helpful for both law enforcement officials as well as the company itself. Importantly, the company must also document its efforts to address the matter. Thorough and real time documentation will also help the insurer respond to the inevitable questions regarding the adequacy of the response to the attack.

Second, the company must also strive to minimize the damage caused by the hack. Damage control includes the preservation of business assets, and may mean weighing whether the cost of taking down a system will cause the loss of data and downtime that is worth the upside of halting a further security breach. The company may also need to prioritize systems for restoration. In both these cases, having already assessed the ''crown jewels'' will aid the company in making these determinations.

Finally, the repair must also prevent further incidents of breach through the same vulnerability. This may mean revisiting the security plan, reassessing vendors and conducting additional audits.

The Plan Should Identify Long-Term Priorities After the Immediate Response to the Breach Has Been Addressed.

As soon as a breach is discovered, one of the highest priorities is to repair the breach. Ideally, this objective can be accomplished quickly after the discovery. However, it is important to conduct further tests, both to ensure the efficacy of the repair and to decrease the chances of another similar incident.

As discussed above, there is a growing body of law concerning the reporting to government and consumers. As the company's understanding of the breach is augmented, it should ensure that the original reporting remains accurate in light of any new information.

And part of any breach response plan must be to consider whether remediation is required or advisable for any affected consumers, and, if so, what form of remediation is both possible and helpful. This means that the company should be tracking the types of remediation that other companies have offered when confronted with their own breaches, public reception to those remedial measures, as well as the types of resources that are likely to be required in order to execute the remediation plan. After a breach, there is a real possibility of multiple lawsuits and class actions being filed against

the company in various jurisdictions. Some states also permit private causes of action for violation of the breach notification statutes. Ideally, the remediation that is devised for the breach will go a long way toward addressing consumer harm and therefore decreases the likelihood of a suit in the first instance, or decreases the possibility of damages for any suit that does proceed.

Following the attack, especially one that draws press coverage, the company should consider how it can best repair any reputational harm with consumers/the general public, with any agents or other entities with whom it does business and also with its own employees. It is possible that new security measures put in place as a result of the breach may lead to a marketing opportunity. The general rule is to communicate early and often, although it is important to be confident of the facts before making any public statements as well as cognizant of any secrecy required due to an ongoing criminal investigation.

Finally, the company should plan a detailed analysis of its response to incident. This is helpful not only for internal purposes, but may also contain information that can and should be shared outside the organization for the good of the business community. In other words, this is a learning opportunity not only for the company, which may identify ways to improve its cyber plan, but is potentially information that the insurer will be able to share with the industry at large.

  PVLR ISSN 1538-3423