IS YOUR CYBER LIABILITY INSURANCE ANY GOOD? A GUIDE FOR BANKS TO EVALUATE THEIR CYBER LIABILITY INSURANCE COVERAGE

THOMAS H. BENTZ, JR.*

I. INTRODUCTION

The last several years have taught many banks that no matter how strong their IT defenses are, no matter how well they train their employees, and no matter how much time or money they spend on network security, they will experience a breach. It is not a matter of if; it is a matter of when.

History has also taught that data breaches are expensive. According to Ponemon, an independent research institute that studies privacy, data protection and information security policy, the average cost of a data breach in the United States in 2016 was $7.01 million, up from $6.53 million in 2015.[1] A data breach may also result in business interruption losses, loss of intellectual property, fines and penalties, and significant harm to a company's reputation.

Banks also make attractive targets for many hackers. Banks, both large and small, have been repeatedly targeted by hackers. In 2015 alone, 795 confirmed data breaches occurred within the financial services industry.[2] Somewhat unsurprisingly, eighty-nine percent of breaches had a financial or espionage motive.[3] The industry has been plagued with recent attacks, resulting in millions of dollars of losses in addition to compromised customer information.[4] In the wake of these

* Thomas H. Bentz, Jr. is a partner at Holland & Knight where he leads the firm's Directors & Officers, Cyber and Management Liability Insurance (D&O) Team. The D&O team provides insight and guidance on ways to improve policy language and helps insureds maximize their possible insurance recovery for Cyber liability, Directors & Officers liability and other management liability insurance policies.1. Ponemon Inst., 2016 Cost of Data Breach Study: Global Analysis 7 (2016).

2. VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 4 (2016).

3. *Id.*

4. *See, e.g.*, Nilesh Christopher, *The Worst Cyber Attacks of 2016*, THE ECON. TIMES (Dec. 28, 2016, 8:59 AM), http://economictimes.indiatimes.com/small-biz/security-tech/security/the-worst-cyber-attacks-of-2016/articleshow/56212448.cms (recapping the

cyberattacks, regulators have placed a heightened emphasis on how banks handle their cyber risk mitigation efforts.[5]

To mitigate their exposure, many banks turn to cyber liability insurance to try to minimize losses in the event of a breach. Unfortunately, cyber liability insurance policies are both complicated and rapidly changing. There is no standard policy form, which means that the coverage offered by one insurer can (and often does) differ dramatically from that offered by another insurer. There is also little agreement among insurers on what should be covered, when the coverage should be triggered, or even how basic terms should be defined. These differences make understanding the extent of a bank's coverage very difficult. It also makes it nearly impossible (or at least foolish) to purchase this coverage based on price alone.

Simply knowing what issues to consider when purchasing a cyber insurance policy is one of the most difficult challenges for banks. The remaining parts of the Article discuss the top five issues a bank should consider when looking for a strong cyber liability insurance policy.[6]

II. KNOW WHAT COVERAGE YOU NEED

There are roughly ten different coverage grants that are

hacking of Bangladesh's central bank in February 2016, which resulted in the theft of $81 million); *see also, e.g.*, Jose Pagliery, *JPMorgan's Accused Hackers Had Vast $100 Million Operation*, CNN (Nov. 10, 2015, 5:27 PM), http://money.cnn.com/2015/11/10/technology/jpmorgan-hack-charges/ (detailing "'the largest theft of customer data from a U.S. financial institution in history,' according to prosecutors"); Can Sezer & Birsen Altayli, *Turkey's Akbank Faces $4 Million Hit From Attempted Cyber Heist*, REUTERS (Dec. 16, 2016, 10:04 AM), http://www.reuters.com/article/us-akbank-cyber-idUSKBN1450MC (reporting an attempted cyberattack on Akbank).

5. *See* Jesse Hamilton, *Bank Cyber Attacks Said to Prompt Fed to Prepare New Safeguards*, BLOOMBERG (July 16, 2016, 5:00 AM), https://www.bloomberg.com/news/articles/2016-07-08/bank-cyber-attacks-said-to-prompt-fed-to-prepare-new-safeguards (discussing potential actions to be taken by regulators and the reasons therefor).

6. *See infra* Parts II–VI; *see also* THOMAS H. BENTZ JR., A BUYER'S GUIDE TO CYBER LIABILITY INSURANCE COVERAGE (Holland & Knight 2015), https://www.hklaw.com/books/a-buyers-guide-to-cyber-liability-insurance-coverage-2015/ ("*A Buyer's Guide to Cyber Liability Coverage* provides a comprehensive review of cyber liability insurance and offers practical, easy-to-understand tips on how to obtain broad insurance protection. This highly informative booklet outlines key provisions that need to be negotiated in a cyber liability insurance policy, as well as tips on claims handling in order to maximize a potential insurance recovery.").

available from most cyber insurers. Different insurers may label these coverage grants differently. Some will combine the grants or split them into different coverage parts with different limits and retentions, and some will only offer a portion of the protections. This lack of uniformity is part of the reason that understanding cyber liability insurance is so difficult.

Knowing what coverage you need as a bank and what is available is essential to purchasing the right cyber policy. The different coverage grants available are described below.

A. Forensic Investigation Coverage

This coverage grant covers the costs and expenses related to determining whether a cyberattack has occurred, how it occurred, and how to stop the attack or loss of data. Some policies also cover work needed to prevent future breaches.

B. Crisis Management Cost

This coverage grant covers crisis management and public relations expenses to assist in managing and mitigating a cyber event. Some policies also cover the costs related to setting up a post-breach call center.

C. Notification or Credit Monitoring Costs

This coverage grant covers costs related to notifying customers and others about a cyber event, as well as any mandatory credit or fraud monitoring expenses. Most policies will cover credit monitoring for one year. Some bank policies will also cover costs necessary to restore stolen identities.

D. Litigation and Privacy Liability Expenses

This coverage grant covers defense costs, judgments, settlements, and related liabilities caused by plaintiffs who bring suit against the insured for various theories of recovery due to the cyber event. Some policies only provide this coverage if there is theft of data, such as when a hacker obtains personally identifiable information.

Other policies will provide this coverage even if there is an intrusion without theft. This is an important distinction for some banks and may result in a significant difference in the coverage provided.

E. Regulatory Defense and Penalties Coverage

This coverage grant covers defense costs to prepare for and defend against regulatory proceedings, including legal, technical, and forensic work. Some bank policies also cover certain fines and penalties that may be assessed against the bank, as well as costs related to responding to government inquiries about the cyber event. Cyber liability insurance is one of the few insurance policies that may cover fines and penalties. This is extremely valuable when dealing with regulators from multiple states that are enforcing different and even potentially inconsistent laws.

F. Online Defamation and Copyright and Trademark Infringement

This coverage grant covers costs related to claims of defamation and copyright and trademark infringement for material published on the bank's website. This coverage is not for losses related to a data breach or intrusion. Instead, it is for improper use of information by the bank: for example, if a bank's website uses a photo of a customer without the customer's permission. This coverage is generally only available for website activities, it does not cover print or other types of media.

G. Network Business Interruption Coverage

This coverage grant covers lost income and operating expenses due to a "material interruption or suspension" of a bank's business caused by a "network security failure." Definitions of "material interruption" and "network security failure" vary greatly between policies. Some policies will only include a data breach, whereas others will also include the introduction of a virus or other type of disruption. The scope of coverage may also vary significantly. Depending on the policy, coverage may be available for: (1) income lost when the bank cannot sell its products because its computer system failed; (2)

dependent business interruption;[7] or (3) extended business interruption. Currently, only a few insurers offer dependent and extended business interruption coverage on their policy forms. Some insurers only offer these extensions by endorsement, and some will not offer the coverage.

H. Expense Coverage

This coverage grant covers certain expenses necessary to expedite recovery from an electronic disruption. Covered expenses are generally fairly limited and subject to lower limits of liability. Some policies only cover these expenses if the expense "reduces" the loss. This can be tricky because it is often hard to know whether an extra expense will reduce the loss at the time the expense is incurred.

I. Data Loss and Restoration Coverage

This coverage grant covers the costs of retrieving and restoring data, hardware, software, and other information damaged or destroyed in a cyberattack. Some policies will also cover damages caused when an employee accidently erases data. This coverage does not apply if the employee acted intentionally. It also does not typically cover costs for upgrading or otherwise improving software during a restoration process.

J. Cyber Extortion Coverage

This coverage grant covers costs related to hackers who attempt to extort money by threatening to release sensitive information or data if a ransom is not paid, as well as costs related to hackers who attempt to hold a network or data on the network hostage. Typically, this coverage will pay for: (1) the money necessary to meet the extortion demand; (2) the costs of a consultant or expert to negotiate with the extortionist; and (3) the costs of an expert to stop the intrusion and block future extortion attempts. This may be extremely valuable coverage because many banks have little or no experience negotiating with extortionists.

7. "Dependent business interruption" covers a bank's losses that result from another party's downtime. For example, if a critical vendor supporting the bank is hacked and, as a result, the bank cannot provide necessary services to its customers.

K. Computer Fraud Coverage

This coverage grant covers losses related to the loss or destruction of a bank's data as a result of criminal or fraudulent cyberattacks. A typical scenario involves a hacker obtaining information about a bank's customer and then using that information to withdraw money from the customer's bank account through an ATM. This coverage grant does not cover fraudulent acts of employees, independent contractors, or persons under the bank's supervision.

L. Improper Electronic Transfer of Funds Coverage

This coverage grant covers lost income and operating expenses due to a material interruption or suspension of an insured's business caused by a network security failure. This coverage grant requires the fraudulent transfer of funds from one financial institution to another. The last two coverage grants are increasingly difficult to obtain in off-the-shelf cyber liability forms.

Not all coverage grants are available to all banks and not all banks will need all of the coverage grants that are available. Banks can save money by only selecting the coverage grants they need.

III. MAKE SURE YOUR POLICIES WORK TOGETHER

Another reason that purchasing the right cyber insurance policy can be so difficult is because there is a lot of potential for overlapping coverage with other lines of insurance. This can be a serious issue as it may affect: (1) which policy applies or is primary in the event of a loss; (2) how losses that are covered under multiple policies will be allocated among those policies; (3) what retention or deductible would apply to a particular claim; (4) which policy determines choice of counsel or other vendors; and (5) what hourly rate will be paid to counsel or other vendors. Any one of these issues may make a significant difference for a claim.

Disputes involving approval of defense counsel and how much defense counsel may be paid are becoming some of the more difficult issues to resolve in a claim situation. Failure to work out these issues in advance can leave a bank paying the difference between the actual expense and the amount covered by insurance. This essentially means

that the bank has co-insurance for its defense costs.

The claims-made requirement of many policies may also present problems for banks in the event of a claim. Different types of policies have varying requirements about when a claim must be reported. Banks are well advised to coordinate their reporting requirements in advance, so they are not attempting to resolve these issues for the first time after a cyber event has occurred.

Some of the ways other types of insurance policies may overlap with a cyber insurance policy are outlined below.

A. Directors and Officers (D&O) Coverage

One of the largest potential exposures in the wake of a cyber event has turned out to be derivative actions against the bank's board of directors for failure to exercise proper business judgment in preparing for or dealing with a cyber event. These types of derivative claims may be covered under a D&O policy. Other third-party claims against the directors and officers of the bank may also be covered by a D&O policy.

B. Errors & Omissions or Professional Liability Insurance (E&O) Coverage

An E&O policy may provide some crossover coverage for a cyber claim. For example, banks have a duty to keep their clients' information confidential. Failure to keep personally identifiable information confidential as a result of a data breach may be covered by a bank's E&O policy. However, some insurers have denied such claims, arguing that a data breach is not caused by a wrongful act by the bank. Regardless, even the broadest E&O policies are unlikely to provide notification, credit monitoring coverage, or full coverage for forensic investigations.[8] As such, a cyber policy will likely be needed for full protection.

8. Recently, some E&O carriers have added limited cyber protections to their E&O policies. Banks should carefully consider whether any additional coverage provided by their E&O carrier will cover all of their risk transfer needs. Often, this additional coverage is not as broad as the protection offered in a standalone cyber policy.

C. Commercial General Liability (CGL) Coverage

Many CGL policies *offered* at least some coverage for a cyber event. For example, many CGL policies covered invasion of privacy or privacy or confidentiality allegations. Recently, however, the standard CGL form was amended to add an exclusion for cyber events. This may limit the amount of coverage available under a CGL policy going forward.

D. Fiduciary Liability Insurance (FI) Coverage

Certain provisions of the Health Insurance Portability and Accountability Act (HIPAA)[9] and the Health Information Technology for Economic and Clinical Health Act (HITECH)[10] require prompt notice of a data breach or privacy event and provide strict penalties for failure to comply with the laws.[11] A strong FI policy may respond to some of the notice expenses, as well as certain penalties from a cyber event. However, as noted with E&O coverage, it is unlikely that an FI policy would cover notification, credit monitoring, or full forensic investigations.

E. Employment Practices Liability Insurance (EPLI) Coverage

EPLI policies may cover certain allegations by employees that the bank failed to protect their personally identifiable information. This is highly dependent on the allegations made by the employees. Some EPLI policies may also provide coverage for third parties. However, these protections are generally only available when the plaintiff can show discrimination or harassment. EPLI policies are also unlikely to cover notification or credit monitoring costs.

9. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections 42 U.S.C.).

10. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111–5, 123 Stat. 115 (2009) (codified as amended in scattered sections of 42 U.S.C.).

11. *Id.* § 13402, 42 U.S.C. § 17932; Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. §§ 164.400–.414 (2016).

F. Crime or Fidelity Coverage

Finally, it may also be possible to find some coverage for a cyber event or data breach under a crime/fidelity policy. Again, this is dependent on the damages alleged. For example, some crime policies will include a computer fraud rider that may allow coverage for certain expenses related to customer communications, public relations, lawsuits, regulatory defense costs, and fines imposed by credit card vendors.

IV. KNOW AND UNDERSTAND THE DEFENSE ARRANGEMENTS

Cyber policies have several unique characteristics that make understanding the defense arrangements both critical and confusing.

A. Duty to Defend

Perhaps the first issue to consider is who gets to control the defense of a claim. Most cyber liability policies are now written on a "duty to defend" basis. This means that the insurer (not the bank) controls the defense and claim strategy. Decisions such as which law firm to use, whether and how to defend a claim, and on what terms a claim should be settled are determined by the insurer in this type of policy.

There may be some real benefits to a duty to defend policy for the right bank. The fact is that many smaller banks are not set up to handle a data breach or other cyber-related claims on their own. Having access to known and vetted experts and professionals in the cyber or data breach fields may save a bank time and money, and may reduce losses or even help prevent future losses from occurring.

However, more sophisticated banks may be uncomfortable with a duty to defend arrangement—especially when the bank's reputation is on the line. For these banks, a non-duty to defend policy is better because it gives the bank more control of the defense of the claim. However, this additional control comes with insurer oversight. The non-duty to defend policy also requires a bank to obtain the insurers' consent prior to incurring defense costs or agreeing to a settlement. Failure to obtain that consent may leave a bank responsible for paying all or a portion of its expenses. In short, although the bank controls the

defense, the bank must still work with its insurers if it hopes to have its expenses covered by the insurance policy.

Banks that have retained their own computer or forensic experts and legal professionals to review or vet their computer systems, apps, and related services may also prefer a non-duty to defend policy. Typically, banks that have retained their own experts in the past will want to use those experts in the event of a claim. Unfortunately, most cyber policies will only provide coverage if the bank uses one of the experts or professionals included on the policy's "panel list." This may be extremely frustrating to a bank. Using a non-panel firm may jeopardize the coverage or even void it altogether.

B. Panel Counsel

This is a common issue for cyber liability policies because cyber liability policies often require the use of a pre-approved or "panel firm" to act as a breach coach, public relations firm, and law firm as a condition for coverage. Many banks are more proactive today in their approach to cyber risk, and many have hired experts and legal professionals to assist them with their planning and crisis management needs. This may create significant issues if the bank is not allowed to use the preferred expert or professional that it has a pre-existing relationship with simply because that expert or firm is not on the pre-approved panel. The time to learn about and resolve these potential issues is before the policy is finalized. Insurers are often much more willing to endorse a coach or firm onto a policy at renewal or before the policy is purchased than to provide an exception at the time of the claim. In addition, the bank will need to respond promptly to a breach and may not have time to seek an exception to the panel firm requirements after a breach is discovered.

C. Beware the "Double Secret" Panel Counsel Requirement

Some insurers will say that a bank may use whatever service provider that it wants as long as the service provider is qualified and its hourly rates are "necessary and reasonable." That may sound attractive, but it is often difficult to find a top service provider that will work for what an insurer thinks is "necessary and reasonable." In a recent

coverage dispute, an insured had three quotes from service providers—the least expensive provider charged $600 per hour. The most the insurer would approve is $209 per hour. The business could not find a service provider that would work for $209 per hour, so it had to either use the firm recommended by its insurer or pay the difference between what the insurer was willing to pay and the amount the qualified vendors it found were willing to charge. This essentially is a secret panel counsel requirement since it is not disclosed and the only vendor willing to work for the amount the insurer considered "reasonable" was the vendor it had pre-selected. To avoid this situation, it is crucial that banks negotiate specific service providers, including hourly rates, into their policies in advance of a claim.

V. NEGOTIATE KEY EXCLUSIONS

Banks are well advised to closely consider the scope of the exclusions in their cyber policies. Small changes in the language can have dramatic ramifications to the coverage. Some examples of exclusions that need to be negotiated on a cyber policy are discussed below.

A. Prior Acts Exclusion

A typical prior acts exclusion excludes coverage for any claim based upon wrongful acts that occurred prior to a certain date (often the inception date of the policy). This can be extremely problematic in the cyber context because cyber-criminals and hackers may install spyware, viruses, and other malware long before a breach is discovered. If the cyber policy considers the intrusion date as the date of the wrongful act, a bank may end up with no coverage for a breach that is discovered after the policy's inception. For this reason, banks should make every effort to avoid prior acts exclusions whenever possible.

B. Laptop Exclusion

Many banks are surprised to learn that cyber liability policies generally exclude coverage for portable electronic devices such as laptop computers or cell phones. Obviously, this can severely limit the coverage provided by a cyber policy. Fortunately, many insurers will

remove this exclusion if a bank agrees to provide "satisfactory" encryption for any data contained on the portable devices—something most banks do already.

C. Bodily Injury or Property Damage Exclusion

Cyber liability policies often exclude coverage for any claim "arising out of, based upon or attributable to" property damage and bodily injury. This is too broad for many banks. Instead, the quoted language should be replaced with the word "for."

This change is important because although a cyber policy is not intended to cover general liability exposures such as bodily injury or property damage, it must still be able to respond to claims based on the breach that do not involve bodily injury or property damage directly—even if such losses were also caused by the breach.

The bodily injury or property damage exclusion should also include a carve back for mental anguish, emotional distress, and shock caused by a cyber event. Plaintiffs may allege these types of damages after a breach of their personal information. Many insurers will only provide this coverage upon request.

D. Mechanical or Electronic Failure Exclusion

The mechanical/electronic failure exclusion removes coverage for claims caused by a mechanical shut down such as when a computer stops working. This exclusion needs to be limited so that if a cyber-criminal causes the mechanical failure or shut down by means of a virus, spam attack, or something similar, the policy may respond.

E. Acts of War, Invasion, and Insurrection Exclusion

Many cyber policies exclude coverage for claims involving events such as acts of war, invasion, insurrection, or terrorism. Including terrorism in this exclusion can be problematic in the cyber context as almost all cyberattacks could be considered acts of terrorism whether foreign or domestic. This is especially true for banks that may be attacked by a nation-state entity. A strong cyber policy should not reference terrorism in this exclusion.

F. Employment Practices Exclusion

Cyber liability policies often exclude coverage for employment practices claims. If a cyber policy has this type of exclusion, a bank should make sure that there is a carve back for employment claims alleging privacy violations caused by a data breach.

G. Employee Retirement Income Security Act (ERISA) Exclusion

Similar to the employment practices exclusion described above, a strong cyber liability policy will have a carve back to the ERISA exclusion for claims alleging damages caused by a data breach of a bank's employee benefits program.

H. Illegal or Fraudulent Conduct Exclusions

Most cyber policies contain exclusions for fraudulent, intentional, and illegal misconduct. How a policy determines whether a conduct exclusion applies, when the determination may be made, and who gets to make the determination is extremely important.

For this reason, many banks prefer a "final, non-appealable adjudication in the underlying action" standard. This standard provides individual insureds with the maximum coverage possible and requires a final, non-appealable adjudication by a court in the underlying action to establish that the alleged wrongful conduct occurred. Without such a final non-appealable adjudication of wrongful conduct, the exclusion does not apply, meaning there is coverage available from the policy.

I. The Insured vs. Insured Exclusion

The insured vs. insured exclusion states that the policy will not cover a claim made by one insured against another insured. However, many cyber liability insurers will agree to "back out" certain insured vs. insured claims for various reasons, including the following: (1) failure to protect confidential information; (2) failure to disclose a breach event in violation of law; (3) the unintentional failure to comply with the insured's privacy policy; and (4) violations of privacy statutes. Often these carve backs only relate to a specific coverage grant, so it is important to review each coverage grant separately.

J. Exclusion Severability

Finally, in order to make sure that the acts of one insured person do not impact coverage for other innocent insureds, a cyber liability insurance policy should contain an exclusion severability provision. An exclusion severability provision states that no wrongful act committed by any one insured shall be imputed to any other insured for purposes of determining the applicability of any of the exclusions.

VI. CHOOSE YOUR INSURER WISELY

Although the most important items to consider when deciding which cyber liability policy to purchase are the terms and conditions of the policy itself, nearly as important is which insurer to purchase from. Never forget that you purchase insurance for the worst-case scenario. You want to have high confidence that your insurer will be a true partner and asset if the worst-case scenario happens.

A. Claims Handling

Different insurers handle claims very differently. Before deciding to purchase a cyber liability policy, it is important to know the insurer's reputation for paying claims. Banks may also find it helpful to know whether the insurer has its own experienced claims staff or whether it uses outside law firms to adjust its claims. Having a knowledgeable and experienced claims staff can be very beneficial for banks. The best insurers act as a resource for their insureds, sharing their experience and helping their insureds navigate a stressful time.

Banks with a global footprint may also want to consider whether their insurers have claims people in the relevant jurisdictions. Knowledge of local laws and customs may be very valuable in a claim situation.

B. Longevity in the Industry

Some insurers try to time their entry and exit from particular areas of insurance to coincide with the hard and soft market cycle. While such an insurer may be able to offer lower prices during "good times," it is typically better for an insured to work with an insurer who

will remain in the market in both good and bad times. Insurers that are committed to a line of coverage typically understand the relationship between the insurer and insured, which is an important part of the coverage.

VII. BONUS TIP: OBTAINING BROAD COVERAGE DOES NOT NECESSARILY COST MORE

Many banks are surprised to learn that adding endorsements and making improvements to their coverage does not often increase their premiums. Some banks have added more than sixty enhancements to their policies without any increase in the premiums. Banks need to take advantage of this fact in order to obtain the broadest coverage possible.

By taking the time to negotiate improvements, banks can greatly improve the chances that their cyber liability policy will protect them when they need it most.