KEY QUESTIONS FOR FINANCIAL INSTITUTIONS SEEKING TO MAXIMIZE INSURANCE FOR "CYBER" RISKS

Lorelie S. Masters, Syed S. Ahmad, and Jennifer White
October 4, 2017

The financial sector is the top industry target for cyber criminals, with phishing, malware and ransomware attacks increasing by double- and triple-digit percentages in the past year.[1] It is also a favored target for government investigations and shareholder suits; indeed, in 2016, securities class actions were at their highest number since the dot-com crash in 2000.[2]

Key Questions

These risks make comprehensive insurance programs imperative, especially with respect to crime and cyber insurance and directors and officers ("D&O") insurance. But merely paying the premium for these policies is not enough to ensure coverage for subsequent claims. Financial institutions must ensure that the terms of these policies address their industry – and business – specific risks. They must also negotiate to avoid common pitfalls in these coverages that may leave financial institutions unnecessarily exposed to loss.

Financial institutions may avoid these hazards by asking a few critical questions at the coverage counseling and policy selection stages.

(1) What Representations were made in the Cyber Insurance Application?

Insurers use cyber insurance applications to gather broad information about companies' cyber-related internal controls, and the extent to which businesses are in compliance with cyber-related policies and procedures. Many applications also ask the prospective insured to warrant that third parties (such as cloud service providers) meet "all security compliance requirements," or that the business has an "up-to-date" firewall and antivirus software in place. Renewal applications, though less lengthy, incorporate the representations made in those prior applications.

How questions are answered at application and renewal may prove critical to coverage in the event of a subsequent claim. As the applications explain, insurers rely on these representations when making the decision to insure. Thus, misrepresentations and omissions can be grounds for rescission of the policy. Courts have granted rescission for even unintentional omissions or failure to qualify or correct application answers.[3] Thus, warranting third-party conduct (over which the principle has no real control) or agreeing that all systems are always "up-to-date" (which may not be entirely accurate, if the IT department is consulted) can get insureds into hot water when cyber protections are breached.

Indeed, cyber insurers are increasingly analyzing the information disclosed at the application stage when considering ways to avoid payment of claims. For example, Columbia Casualty Company refused to cover the settlement of a data breach class action based on the claim that its insured, Cottage Health Systems, failed to "continuously implement the procedures and risk controls identified in its application."[4] The disputed answers were to questions like, "Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes?" and "Whenever you entrust sensitive information to third parties, do you perform due diligence … to ensure that their safeguards for protecting sensitive information meet your standards?"

Financial institutions are particularly at risk of rescission because of the large size of potential losses (which insurers are less interested in paying) and because of the financial industry's increasing reliance on third-party vendors, who touch everything from customer controls to actual fund transfer. To avoid these coverage battles, businesses must err on the side of full disclosure at the application stage and revisit original applications at renewal to update or qualify answers as appropriate. Also, key business and technical personnel (such as IT and HR) should help prepare cyber insurance application responses.

(2) Is the Company Adequately Protected in the Event of a Regulatory Investigation?

Hackers are not the only group targeting the financial sector. Financial institutions also have become a growing target for regulators pre- and post-breach. For example, on March 1, New York became the first state to impose certain cybersecurity minimum requirements on banks and financial institutions licensed to operate in the state (subject to certain exemptions).[5] Increased scrutiny at the state level merely piggybacks on preexisting focus of the Securities and Exchange Commission, among other federal enforcement arms.[6]

To withstand the increased attention, financial institutions should purchase adequate coverage to address fines and penalties and settlements with local, state, federal and foreign enforcement bodies. Importantly, this coverage should not depend on "formal" enforcement activity because government organizations have broad authority to investigate "informally." The practical impact on the business is virtually indistinguishable. As such, financial institutions should explore enhancements to address the costs related to "informal" investigations, the availability of which will be largely dependent on the insured's market power.

(3) Will the Financial Institution's Other Policies Pick Up "Cyber" Losses?

Cyber insurance is one piece of the cyber risk insurance portfolio. Another important piece is crime insurance. Standard endorsements to crime policies now address different types of what most businesses consider to be "cyber risk," such as when an online criminal impersonates a legitimate vendor or company executive to trick an employee into wiring company funds to an offshore account (commonly called "social engineering fraud").

When crime policies lack social engineering endorsements, coverage may be found under standard crime policies—but whether coverage will apply varies broadly depending on the nature of the fraud, the policy definitions, the policy exclusions and the jurisdictions. For example, courts are split on the role fraudulent emails must play in effecting fraudulent funds transfers. In *Medidata Solutions, Inc. v. Federal Insurance Co.*[7] and *Principal Solutions Group, LLC v. Ironshore Indemnity Inc.*,[8] the courts found coverage based on precipitating emails wherein the criminal impersonated a high-level corporate officer seeking money related to a legitimate corporate acquisition. The courts found that the fraud would not have occurred but for the electronic communications. But in *Apache v. Great American Ins. Co.*[9] and *American Tooling Center, Inc. v. Travelers Casualty & Surety Company of America*,[10] the courts found that emails were too attenuated from the loss; in Apache, the court thought it relevant that the scheme started with a phone call, as opposed to an email, and in American Tooling, the court blamedfailure to follow internal controls as opposed to the technology. The different outcomes of these cases underscore the importance of understanding how traditional policies may or may not respond to "cyber" losses so gaps may be filled through other insurance, or by endorsement.

Financial institutions may also find cover for criminal activity under financial institution bonds. For example, last year, the U.S. Court of Appeals for the Eighth Circuit found a bank covered for $485,000 in fraudulent wire transfers achieved by a Trojan horse virus after an employee inadvertently left physical tokens in a bank computer, which were part of the multipronged wire transfer approval process.[11] The bank's insurer denied coverage based on numerous exclusions associated with a common theme: that employee negligence broke the causal chain between third-party criminal acts and otherwise covered losses. However, the court found the loss covered by the policy, holding that "[e]ven if the employees' negligent actions 'played an essential role' in the loss," the "overriding cause" was the criminal acts, without which there would have been no intrusion into the system or subsequent wire transfer.

(4) Does the Business have Sufficient Coverage to Protect its Directors and Officers from Litigation Resulting from Cyberattacks?

After Target reported that cyber criminals had stolen the customer credit card details and personal information of approximately 40 million customers, Target's shareholders sued Target's directors and officers for failure to take action that would have prevented the breach. Shareholders alleged that Target's board knew point-of-sale machines were vulnerable to attack, but failed to update the systems, and knew about other security vulnerabilities.[12] Equifax is now the subject of similar suits.[13]

Many D&O policies will not pick up the exposure caused by data breaches, because traditional D&O policies contain cyber liability or "invasion of privacy" exclusions that otherwise limit coverage. Even where "cyber" exclusions are absent, insurers may seek to avoid coverage using other exclusions, like regulatory exclusions (which would include many types of enforcement actions) or bodily injury exclusions (which usually include allegations of "emotional distress" or the "right to privacy").

There is considerable risk in allowing these gaps to go unchecked. Although shareholder suits have been unsuccessful to date, the expense associated with defending such complex litigation can prove astronomically expensive. Financial

institutions should negotiate to eliminate, or carve back, overly broad cyber-related exclusions.

(5) After a Breach, Who Else May be Held Responsible for the Company's Losses?

When customer information is exposed due an attack on a vendor, a financial institution should also consider whether its vendor's insurance policies will address the financial institution's exposures. Ideally, financial institutions should require its vendors—as part of the service agreement—to obtain and verify certain types of coverage, at certain coverage levels. In certain situations, it may be appropriate to become an additional insured under the vendor's policies as well, which may require further negotiations to remove common provisions like the insured-versus-insured exclusion.

Even when losses are not indemnified pursuant to contract, or paid to the financial institution as an additional insured, financial institutions may still recover insurance proceeds, indirectly, in litigation against the vendor. For example, after Chipotle's data breach exposed bank and credit union customers' names and card numbers, the financial institutions sued the restaurant giant for lax security that caused the institutions to incur costs to "cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage."[14] Shifting loss through litigation may prove necessary, especially where business insurance does not respond appropriately to financial institution losses.

Conclusion

Financial institutions maintain considerable personally identifiable information, and private information, about their customers, and are involved in the exchange of millions of dollars every day. Protecting that information through tight internal controls, technological safeguards and honest vulnerability analysis and patching are important parts of the battle against cyber criminals. Insurance, too, plays an important role in mitigating that risk, if properly tailored to the needs of the institution using it.

Endnotes

[1] http://assets.metricstream.com/pdf/industry-reports/state-cyber-security-financial-services-industry.pdf.

[2] https://corpgov.law.harvard.edu/2017/02/10/2016-year-end-securities-litigation-update/.

[3] *HJ Heinz Co v. Starr Surplus Lines Insurance*, No. 16-1447 (3d Cir. 2017).

[4] *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2: 15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015) (dismissed without prejudice because policy included mandatory ADR provision).

[5] *See generally* http://www.dfs.ny.gov/about/press/pr1702161.htm.

[6] https://www.sec.gov/news/pressrelease/2016-112.html.

[7] S.D.N.Y. July 21, 2017.

[8] N.D. Ga. Aug. 30, 2016.

[9] 5th Cir. 2016.

[10] E.D. Mich. Aug. 1, 2017.

[11] *State Bank of Bellingham v. Bancinsure Inc.*, No. 14-3432, (8th Cir. May 20, 2016).

[12] *Davis, et al. v. Steinhafel, et al.*, No. 14-cv-203 (D. Minn.).

[13] https://finance.yahoo.com/news/levi-korsinsky-llp-announces-notice-202900987.html.

[14] *Bellwether Community Credit Union v. Chipotle Mexican Grill Inc.*, No. 1:17-cv-01102 (D. Colo. May 4, 2017).

About the Authors

Lorelie S. Masters and **Syed S. Ahmad** are partners and **Jennifer White** is an associate with the insurance coverage practice at **Hunton & Williams LLP** in Washington. The authors may be reached at lmasters@hunton.com, sahmad@hunton.com, and jewhite@hunton.com, respectively.

For more information, or to begin your free trial:

- Call: 1-800-543-0874
- Email: customerservice@nuco.com
- Online: www.fcandslegal.com

FC&S Legal guarantees you instant access to the most authoritative and comprehensive insurance coverage law information available today.

This powerful, up-to-the-minute online resource enables you to stay apprised of the latest developments through your desktop, laptop, tablet, or smart phone —whenever and wherever you need it.