Insights: Alerts

Cyber Attacks: Is Your Bank Insured?

JANUARY 12, 2015 Written by Edward G. Olifer

State and federal banking regulators' recent focus on cyber security and cyber insurance underscores the importance of procuring cyber insurance, both as a risk management tool and for purposes of demonstrating regulatory compliance. As such, it is imperative that financial institutions review their cyber security insurance policies carefully to ensure that the scope, limits, and sublimits of the coverage are appropriate. Consistent with other areas of risk mitigation, the amounts of such cyber security insurance coverage should be commensurate with the level of risk involved with the bank's operations and the type of activities to be provided. Banks should also understand that not all cyber-insurance products are the same – the scope of coverage can vary drastically among products offered by insurance carriers.

On December 3, 2014, in prepared remarks, Sarah Raskin, Deputy Secretary of the Department of Treasury, highlighted the developing focus of cyber security insurance, stating, "I have been asking our insurance and cyber experts at Treasury to think about how to encourage an environment where market forces create insurance products that enhance cybersecurity for businesses. Ideally, we can imagine the growth of the cyber insurance market as a mechanism that bolsters cyber hygiene for banks across the board."

Most recently, on December 10, 2014, the New York Department of Financial Services (the "NYDFS") issued a guidance letter to all NYDFS-regulated banks outlining the issues and factors on which banks will be evaluated during new targeted, cyber security preparedness assessments. The guidance letter specifically stated that the NYDFS will focus on "[c]yber security insurance coverage and other third-party protections."

Other bank regulators over the last year have issued similar pronouncements. In addition to the extrinsic motivation of the evolving regulatory landscape, banks should also be motivated by the financial and reputational risks of privacy breaches. The 2014 Ponemon Study indicates that the cost of data breaches is increasing. The companies involved in the study reported an average of $201 per record breached, and an average of 29,087 records per breach – that's an average cost of $5,846,487 per breach for the companies studied. For the financial industry (globally), the average costs per breach are higher, at $206 per record, according to the Study.

Cyber-insurance is a concept, not a product, so it is unclear what criteria regulators will use to evaluate banks' cyber-insurance, particularly in light of the rapidly changing cyber-insurance market. At a minimum, banks should be aware that their traditional insurance (e.g., commercial general liability and D&O) likely will exclude coverage for privacy breaches in the near future. Some coverage may be found in a bank's financial institution bond or E&O policies. In addition, most banks have by now purchased some form of stand-alone specialty cyber product, and regulators likely will deem that a necessity. However, there currently is no such thing as a "standard" specialty cyber policy, so it is unclear whether regulators will deem the mere purchase of a cyber policy as sufficient to meet their standards. Therefore, banks should consider evaluating at least three variables that impact the amount of cyber-insurance they carry: the risks insured; the losses insured; and limits/sublimits.

Risks Insured

Data security experts will use technical terms like "DDOS," "mobile malware," "spear-phishing," and others, but the risks

basically break down into the following four categories that should guide banks' cyber-insurance evaluations:

1. The "Oops" – negligent breaches, caused by you, an agent, or a vendor, inadvertently causing a breach.
2. The "Hacker" – intentional attacks/breaches, with the goal of making money, or a statement, by causing or threatening to cause your organization or its customers harm.
3. The "Blogger" – intentional or unintentional, where a blogger or webmaster uses trademarked or copyrighted material, or invades the privacy of a third party without permission. This is traditionally the realm of "media liability" and sometimes "advertising injury" insurance.
4. The "Ghost in the Machine" – some sort of inherent flaw or hole in your hardware or software causes data loss or a security breach.

Losses Covered

Losses arising from cyber risks tend to fall into one of two general categories – "first-party" losses (the bank's direct costs) and "third-party" losses (liability losses). First-party losses consist of costs directly incurred by the bank as a result of the breach, such as costs incurred in connection with privacy notifications, public relations efforts, forensic investigations, restoration of data, and business interruption, and, in some instances, ransom payments. Third-party losses are liability losses, and include defense costs and indemnity payments in connection with customers' claims for damages and regulatory investigations. While other types of insurance policies may or may not cover regulatory penalties, banks' cyber-insurance should cover all of these potential losses but the policy language should be reviewed carefully to determine the types of losses that are covered and those that are excluded. Also, beware of policy language that purports to provide the carrier the unilateral right to determine whether certain costs will be deemed necessary and thus covered. Some policies, for example, state that they cover first party costs that are necessary "in the sole discretion of the insurer." Banks may be able to negotiate language that permits more flexibility and even-handedness should a cyber event occur.

Limits

As with other insurance products, aggregate limits for specialty cyber-insurance will be a function of insurance carrier capacity/risk tolerance, and the premiums that insureds are willing to pay. Excess insurance, attaching at higher losses at a reduced ratio of premiums/limits, may be available to some institutions. However, the most important factor banks should consider is whether their cyber-insurance products provide sufficient limits for the various losses they might incur. For example, many bank policies have drastically lower sub-limits than their aggregate policy limits for certain first first-party losses, when it is the first-party losses that can often be greater than the third-party liability.

Bottom line, cyber risks and costs are increasing for the financial industry (as well as most, if not all, other industries), and cyber risks are evolving more quickly than the cyber-insurance products available on the market. We advise banks to work with their brokers, coverage attorneys, and IT professionals to analyze their risks and whether they have sufficient insurance to cover them, so that when the regulator shows up for the examination, they are ready.

Related People



Edward G. Olifer
t 202.508.5852
eolifer@ktslaw.com