TECH INSIGHTS

Cybersecurity: What Lenders Need to Know

BY BRIAN ALLEN AND THOMAS DEMAYO

BRIAN ALLEN
PKF Clear Thinking

THOMAS J. DEMAYO
PKF O'Connor Davies Advisory LLC

Business disaster is only a click away. Cyberattacks are becoming an epidemic affecting all businesses. A single mishap can critically impair business operations or even shut down operations entirely resulting in catastrophic financial and reputational damage.

Cyberattacks have been steadily increasing as well as getting more sophisticated and the challenge for companies to thwart these attackers continues to evolve. Business exposure has increased with more of the labor force working remotely, creating more entry points for intruders to exploit systems and get access to a company's information and system resources.

According to the FBI Internet Crime Report 2022[1], the potential loss has grown from $6.9 billion in 2021 to more than $10.2 billion in 2022. And while ransomware incidents have decreased, many attacks go unreported.

What Companies Are Facing

For businesses, cybercrime can include any of the following:

- Theft of financial and intellectual property or sensitive information of an individual that can be sold and used in other cybercriminal activities.
- Cyberextortion, such as ransomware, where attackers install malicious code that encrypts company data, preventing the owner from accessing their data unless a ransom is paid for the encryption key. Another common form of extortion is the exfiltration of company data and a threat to make that data public unless the ransom is paid. Often, the attack will include both encryption and exfiltration, further increasing the pressure on the company to pay the ransom.
- Diversion of funds through manipulated e-mails that result in the change of electronic payment instructions.
- Denial of service attacks that result in company systems being overwhelmed and unable to process legitimate business transactions.

What Companies Should Do

For a company to prepare successfully for and defend against the cyber threat, it must establish a cybersecurity program that includes a core competency and capability in the five pillars of information security: Identify, Protect, Detect, Respond and Recover.

As companies evaluate their security programs and look to align with the five pillars, below are some of the key controls they should consider:

- Establish a cybersecurity committee. Effective governance and a philosophy of security that resonates from the top down is critical in the success of a cybersecurity program.
- Perform ongoing risk assessments and more technical exercises, such as penetration testing to evaluate the cyber defenses and response capabilities of the company.
- Perform effective due diligence on any third party that will store, process, transmit or have the potential to impact the security of the company.
- Establish a cybersecurity awareness program. Educate

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

employees on cybersecurity threats and the identification of phishing e-mails. Ongoing phishing testing should be part of the overall awareness training program.

- Enforce strong logical access controls, such as robust passwords and multi-factor authentication. Multi-factor authentication (MFA) should be utilized consistently for access to remote systems or applications that contain data of value and for any privileged access to a system or application.
- Restrict access to only what is needed for an individual to perform their assigned duties. Further, restrict access to not just the user, but also the device from which the user is connecting.
- Employ next generation anti-virus software, known as Endpoint Detection and Response platforms.
- Install vendor-provided security patches on a consistent and timely basis relative to the risk of the vulnerability the patch is intended to fix.
- Collect, analyze and store security logs from all critical systems, network devices, and applications. Alert on known security threats or anomalous activity.
- Implement a backup strategy that is ransomware resilient so that in the event of a ransomware attack, a backup of last resort exists.
- Be resilient. Establish and maintain an incident response, business continuity, and disaster recovery plan.
- Test the plans to ensure they will work as designed and employees fully understand their roles as part of the plans.

Phishing attacks against banking systems have been on the uptick as well. They occur when a threat actor poses as a trusted person or organization to convince individuals to share sensitive information or to send money. Information often includes bank account or credit card information and can be used to make unauthorized purchases or commit bank wire fraud.

Cybersecurity Insurance

Companies can mitigate financial damage with cyber insurance and while it can provide some reimbursement for damages, it can't prevent intrusions from occurring so it's not a replacement for effective IT systems management.

Cybersecurity insurance coverage is on the rise, but in one recent survey, only 19% of organizations claimed to have coverage for cyber events beyond $600,000 and only 55% of organizations claimed to have any cybersecurity insurance at all.[2]

Cyber insurance is still a relatively young product and is going through rapid change as the carriers adjust to loss history and are still working around the edges of a highly unpredictable liability to make it a profitable business. The cost of coverage has been going up too and many firms view cyber coverage as a luxury.

Companies need to do proper planning to understand what their risks are and which cyber insurance products best fit their needs. This should all be done in the context of what the current internal risk management looks like and where it may be necessary to shore up its defenses. Policies are varied and may or may not include a provision for ransomware payments. Most policies will pay for network security, legal and forensic professionals, as well as the costs of restoring data and those necessary to get operations back up and running.

There are generally two types of loss liability — first-party and third-party — and policies may cover one or the other, or both.

First-party coverage typically includes reimbursement for investigations, IT forensics, risk assessments, loss of revenue due to business interruption and costs incurred for data breaches, including customer notification and credit monitoring for example. First-party coverage may also include ransomware payments to extortionists to enable the company to get its data back.

Third-party, also called cyber liability coverage, insures

[2] https://networkassured.com/security/cybersecurity-insurance-statistics

for damages the company may be blamed for and generally include coverage for costs of legal proceedings, settlements, and regulatory fines, for example.

A recent survey by the CRC Group, a wholesaler of specialty insurance, indicates that the minimum standards of underwriting cyber policies include affirmative controls, such as multi-factor authentication (MFA), endpoint detection, backup strategies and email security filtering. In addition to requiring more controls by the insured, many carriers are imposing sub-limits and, in some cases, introducing other exclusions to control their exposure. All this means that careful attention should be paid to obtaining the appropriate cyber policy and understanding the actual coverage and any limitations.

What Lenders Need to Know

Lenders, just like any other business, have to be on guard to protect their information and they are not immune to vulnerabilities with their customers either. A ransomware attack can impair or shut down a customer's business operations entirely and even put a company out of business. Paying a ransom does not guarantee data will be retrievable or that adverse data loss or exposure can be reversed.

Medium- and small-size businesses are at the greatest risk of becoming victims of cybercriminal activity. They don't typically have the resources and sophistication of larger enterprises and are often more vulnerable. A smaller business may very well be unable to pay a ransom or cover uninsured losses if they have insurance coverage at all.

Phishing attacks against banking systems have been on the uptick as well. They occur when a threat actor poses as a trusted person or organization to convince individuals to share sensitive information or to send money. Information often includes bank account or credit card information and can be used to make unauthorized purchases or commit bank wire fraud. These acts can be costly to lenders and put them at reputational risk. Borrowers' information that is hacked can be used by criminals to get fraudulent access to bank funds in the lender's accounts.

Lenders should include in their customer risk analysis a general understanding of their customer's business and general controls around cybersecurity. In some cases, lenders or potential lenders may require a security audit to help a company determine where there may be weaknesses in a company's IT systems.

Brian Allen is a partner with PKF Clear Thinking and has over 25 years of experience serving in controller and CFO positions with both public and private companies. Over the past 15 years, Allen has been engaged by numerous companies in the consumer electronics, beverage, nursery, media, furniture, printing, consumer product, retail, and manufacturing industries to improve financial operations and performance with strategic and financial alternatives, and to serve in interim senior financial positions. During his career, he has had direct responsibility for the accounting, finance, treasury, information technology, real estate, and investor relations functions. Prior to joining PKF Clear Thinking, Allen owned a financial advisory practice with a focus on middle market, consumer product businesses. He can be reached at ballen@pkfct.com.

Thomas J. DeMayo is a partner with PKF O'Connor Davies Advisory LLC. He leads the Firm's Cybersecurity and Privacy Advisory Group and is responsible for the implementation and design of cybersecurity and privacy related services, internal and external audit programs and testing procedures. He focuses on services relating to threat and vulnerability management, governance, privacy, incident response, business continuity, disaster recovery and computer forensics.

He has 20 years of experience with securing and managing information risk across a wide range of industries including commercial entities, hospitality, not-for-profit, governmental, healthcare, private schools and higher education. DeMayo is also a computer forensic specialist and can assist with the acquisition and analysis of data in a forensically sound and legally approved manner.

DeMayo specializes in the areas of information threat and vulnerability management, PCI-DSS compliance, SOX 404 IT Controls, HIPAA, COBIT, and ISO 27001. He has helped many organizations achieve their compliance obligations through intensive and meaningful compliance gap analysis, cyber and information security risk assessments, privacy assessments and penetration tests. Tom has also made numerous presentations on cybersecurity before client and industry groups and has written extensively in this area. He can be reached at tdemayo@pkfod.com.