

Mitigating Borrowers' Cybersecurity Risk

BY BRIAN RESUTEK

Financial and collateral review? Check. Appropriate lender agreements, carveouts and lien perfection? Check. Review of borrower's cybersecurity policies and procedures? Can you repeat that? When it comes to lender due diligence and documentation, organizations are well versed with modeling, credit procedures and deal structures; however, there is a continually growing blind spot that lenders cannot afford to ignore: Cybersecurity.



Simply stated, the cybersecurity risk across a company or borrower should be evaluated by every lender to ensure capable protection levels across computers, networks, programs, and operations at the borrower level. If not evaluated, a cybersecurity breach could severely affect the stability and lifespan of an entity, despite all other underwriting criteria being met. This potential risk of loss is considerable regardless of the size of the business, and unfortunately, the likelihood of an attack is also high adding to the importance.

According to Cybint Solutions, 64% of companies worldwide have experienced at least one form of cyber attack in the past year. While the reasons vary as to why hackers want to attack companies, one fact is certain: The cost to companies is high when a breach occurs. Per IBM's recent 2022 cost of a data breach report, the average cost of a data breach in 2022 was \$4.35 million. While companies such as Equifax and Target made major headlines for their massive breaches, a large majority go unreported to the public, with an even larger figure today likely brewing inside companies (and our borrowers); waiting to be exposed.

207 Days. That was the average time it took for a company to just identify a breach in 2022 per the IBM report. Tack on an

Whitney Schickling, area senior vice president at Gallagher, shared similar guidance for lenders in that a lender's contracts and applications should contain questions on cyber risk and require maintaining a cyber risk policy as a condition. "Every company should feel confident that their data is being managed with proper controls and safeguards in place."

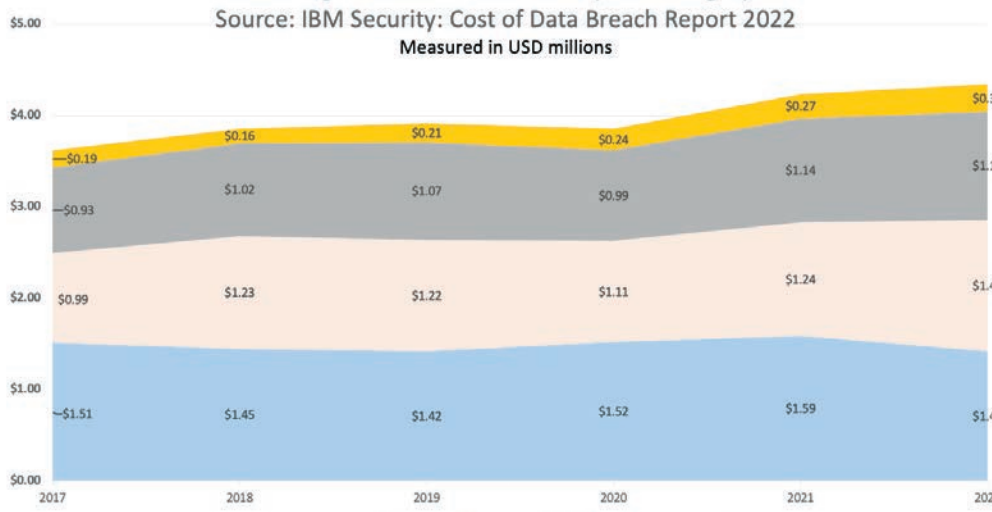


When specifically asked about how SMBs should be evaluating cyber insurance, given limited company resources, Schickling responded, "Cyber insurance has evolved so that it is not just simply a risk transfer. Rather, it enables insureds to have access to cyber experts including vendors, lawyers, forensic specialists and security consultants. Many insurers have platforms to offer external vulnerability scans, phishing trainings and much more. For a small business, it is important

BRIAN RESUTEK
Rosenthal & Rosenthal

to partner with a broker who is knowledgeable of the cyber market and services that are available." The last statement should not be glossed over as small businesses are, unfortunately, a favorite target. Forbes reported that in 2022, 43% of cyberattacks targeted small businesses and that only 14% of small businesses have proper defenses against such attacks. What should also make lenders nervous is that Forbes reported that 83% of small businesses are not financially prepared to recover from such attacks. A Devolutions

Average cost of a data breach by cost category
Source: IBM Security: Cost of Data Breach Report 2022
Measured in USD millions

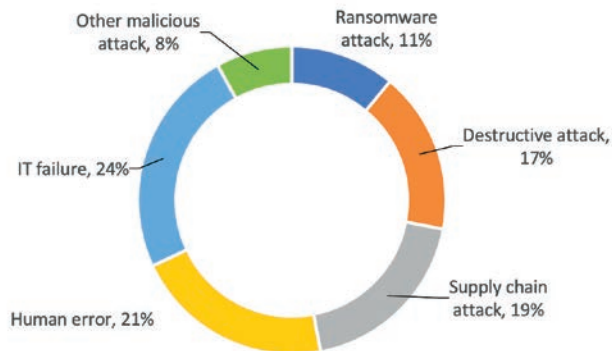


additional 70 days to contain the breach and the full duration is 277 days from start to finish. Ralph Pasquariello of Snellings Walters Insurance Agency emphasizes this point to his clients. "Cybersecurity is the biggest question and threat on the CFO plate today. You need to know what the effect will be to your business when you are down." Pasquariello further cited the importance of appropriate benchmarking to determine limits and understanding how all of a company's insurance policies, such as crime and property, must work in conjunction with a cyber insurance policy. Additionally, lenders should be asking these questions along with what types of procedures, assessments and protocols are in place, along with the frequency of testing.

2021/2022 report came to a similar conclusion with a larger SMB data set. This report indicated that 60% of SMBs go out of business within six months of experiencing a serious cyberattack.

The good news is that there is plenty of help and resources already available to both lenders and borrowers. Many companies utilize both internal and external sources to help combat and manage cyber risk. Kevin Yenglin, director of information security at Rehmann Corporate Services, professional advisory firm that provides accounting, assurance, business solutions and specialized consulting among other services, is one of the resources companies engage with, as Rehmann has a specialized group dedicated to cyber risk. Yenglin agreed that companies need

Types of Breaches Experienced by Organizations



Source: IBM Security: Cost of Data Breach Report 2022


to partner with experienced insurance professionals to evaluate their needs. While coverages are specific and vary by company and need, Yenglin outlined the key coverage areas lenders and businesses should consider:

1. *Cyber Liability Insurance* – Insurance designed to protect businesses from liability arising from data breaches, cyber attacks, and other similar incidents. Typically covers costs such as legal fees, notification costs, and credit monitoring for affected individuals.
2. *Ransomware coverage* - Ransomware attacks have become increasingly common in recent years, and the costs associated with these attacks can be significant. Ransomware insurance can cover costs such as ransom payments, lost income, and the cost of restoring data and systems.
3. *Data Breach coverage* – Breach coverage will help cover attorney fees, forensics, hacker damage, notifications, credit monitoring, and regulatory fines.
4. *Loss of Funds* – This coverage will help cover wire fraud, cyber crime, and social engineering fraud.
5. *Third-party coverage* – This coverage will help cover costs that come from clients, vendors, or regulators. Think of it like someone who wants to take money from your business for an incident.

Operating while “under attack” is perhaps one of the scariest scenarios that a business and their lender potentially face, and where the importance of planning and protocols must be understood in advance. Yenglin mentioned the importance of developing a Cyber Incident Response Plan. This plan outlines the steps to be taken in the event of a cyberattack or other security breach. The plan should also include roles and responsibilities of key personnel, protocols for data backup/recovery, and internal communication procedures along with external communication to stakeholders such as customers, suppliers, and regulatory authorities. Additionally, once the plan is in place, it must be regularly tested and updated as well as communicated to the necessary key personnel and stakeholders.

Email Is Still the Primary Gateway

While many of the policy procedures might reside with key management, most of defense or prevention still remains at the employee level, which is why training and education is so important. E-mail entry remains the key gateway of choice of hackers. Pasquariello mentioned that Business Email Compromise (BEC) remains the most popular route with the average time being over 200 days before a company detects the breach. Literally, a non-authorized individual is lingering inside a company’s firewalls as the company believes they are operating in a secure and “normal” basis as the hacker gathers data, passwords and critical information as they remain undetected. A recent Deloitte study cited that email is responsible for 91% of all cyber attacks. The reason is that corporations still rely on email as the preferred communication method and email invites human error, which can nullify other cyber defense systems. As a result, lenders and companies should be diligent and cognizant that employee training at all levels is being done on a continual basis.

While no lender can guarantee collateral and cash flow performance with absolute certainty in the underwriting process and no company is completely immune or “fully protected” from cyber risk exposure. Lenders though, should be taking actions on their initial underwriting and in loan review sessions thereafter, to understand and evaluate what risks their borrowers face from cyber risk and how these are being mitigated. Lenders should be prepared to have these same questions asked of their organizations as cyber risk and managing its exposure is of major importance in a lending relationship among all parties. 

Brian Resutek is a senior vice president and business development officer for Rosenthal & Rosenthal’s Southeast office in Atlanta, GA. He can be reached at bresutek@rosenthalinc.com.