Cyber Diligence: How to Vet Your Borrowers

By Erik B. Weinick of Otterbourg P.C. and Sherri Davidoff of LMG Security

Editor's Note: Following the article are some important cyber-security and privacy term definitions and FAQ's.

A transportation company is stopped in its tracks for days, due to a company-wide ransomware infection. A mom-and-pop restaurant is hit with nearly $100,000 in fines upon discovery of a payment card data breach. A law firm has $100,000 wired out of its bank account because the bookkeeper clicked on a link in a phishing email.

These are just a few real-world cases where cybersecurity issues can have a direct and negative impact on your borrowers' operations and cash flow, and even impact a borrower's ability to repay their loan. Therefore, credit professionals should consider cyber due diligence and monitoring to be a fundamental component of standard underwriting and credit evaluation processes.

Cause for Concern, a Case Study: Maine Indoor Karting

Many small business owners may think they are immune to a cyber attack because the perpetrators of such attacks are either state actors looking to break into national security agencies, or are sophisticated criminals looking to steal millions of dollars from Fortune 500 companies. Unfortunately, Rick Snow, the owner of an indoor go-cart track in Scarborough, Maine knows differently. According to published reports, he recently clicked on a link in a phishing email and he found himself not in a go-cart race, but in a race to stop criminals from draining the bank accounts holding the cash he needed to pay his employees. While Mr. Snow's initial efforts seemed to be successful (upon realizing the error in clicking on the link in the phishing email, he rushed to close his accounts), the attackers were patient, and two weeks later emptied his new accounts of almost $40,000 in payroll funds.

Mr. Snow is not alone. According to various studies, at least 40% of all cyber attacks target small businesses, and of those, nearly 60% go out of business within 6 months of a cyber crisis. See Mansfield, Matt. "CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know." *Small Business Trends*. N.p., 03 Jan. 2017. Web. 14 June 2017. https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html.

These figures are not surprising considering that the National Center for Middle Market (NCMM) reports that *more than half of* U.S. middle market companies lack an up-to-date strategy to combat the cyber risks they face, and *one-third* concede that they have no cyber action plan at all. See "National Center for the Middle Market Launches Cybersecurity Resource Center" ABL Advisor December 15, 2016. Those are just the numbers based on admissions by businesses to the study's authors, and in reality, the percentages are likely higher.

Cyber Diligence: What Questions Should a Prudent Lender Ask Borrowers?

Assessing your borrowers' cybersecurity risk can seem like a daunting task – but it does not have to be. Many lenders tackle the challenge by developing their own long list of cyber risk assessment questions, or paying for assessments of key borrowers. However, there is often a more efficient way that will save both time and effort. In short, lenders can look to objective measurements of cybersecurity and then common cybersecurity assessment reports, or for smaller and less sophisticated borrowers, lenders can ask tailored questions that can still reveal important information.

Objective Measurements

Russ Cohen, Vice President for Cyber Services at Chubb, developed a new model for assessing cyber risk called "Cyber COPE," which is a transformation of the classic "COPE" assessment methodology.[1] For traditional property insurance, underwriters often assess the "Construction, Occupancy, Protection and Exposures" of a building. In the cyber world, Cohen has transformed the first two categories into "Components" and "Organization."

According to Cohen, the "Components" category includes sample data elements, such as "number of endpoints and network connections, software versions, and data center locations." Questions that lenders may ask in this category include:

[1] Cohen, Russ. "CyberCOPE: Transforming Cyber Underwriting," Chubb

©2017 Credit Research Foundation

- How many computers, laptops and mobile devices do you have?
- How many user accounts exist?
- How many third-party vendors do you rely upon for IT functions?

The "Organization" component, according to Cohen, includes sample data elements, such as the borrower's "industry, quality of IT and security related policies, and use of industry standards." Questions that lenders may ask in this category include:

- What is the borrower's industry?
- Where does the borrower operate geographically, and what obligations (including international) does it incur as a result?
- What information security standards and regulations apply to the organization?
- Has the borrower adopted a formal information security management framework?

The borrower's responses to these questions will reveal a great deal about the level of cyber risk it faces, and will begin to tell the story of what the borrower has done to address that risk.

Request Common Cybersecurity Assessments Reports

After understanding the borrower's objective measurements, the next step is assessing the existing level of *protection* and *exposures*.

Many borrowers are already required to conduct cybersecurity controls assessments, technical testing (such as penetration tests), and risks assessments. These requirements can be pushed down by industry regulators (such as the Office of Civil Rights for health care), vendors (such as the Payment Card Industry (PCI) card brands), or customers who conduct supplier vetting. Since many borrowers have already been subjected to cybersecurity diligence by their own regulators, vendors or customers, they may already have standard reports at the ready that will help you assess their risk. You may want to begin by requesting that your borrowers submit the following three pieces of documentation, if available:

1. **Cybersecurity controls assessment.** This is an evaluation on a common *cybersecurity controls framework*. It is sometimes called an "information security controls assessment" or a "gap assessment."

   A cybersecurity controls framework is essentially a checklist for an organization's cybersecurity program. It can include tasks such as "conduct cybersecurity awareness training" or "perform vulnerability scans." The most important thing to remember is to require borrowers to pick a *widely accepted cybersecurity controls framework* to use for their reports. In the United States, the NIST Cybersecurity Framework is widely used. The ISO 27001 standard is popular for international organizations. By choosing a popular controls framework, you avoid reinventing the wheel and can easily compare borrowers' profiles.
2. **Technical test results**. Does reality match what is on paper? Regulations such as HIPAA and industry standards such as PCI-DSS already require borrowers to conduct technical cybersecurity testing. Ask to see a letter of attestation or summary of the borrower's penetration test or vulnerability assessment results. Make sure technical cybersecurity testing is conducted by a qualified third-party that did not set up the borrower's network, to ensure separation of duties.
3. **Risk assessment and risk management plan.** A formal risk assessment should take into account both the results of cybersecurity controls assessment and technical testing. Again, it is wise to ask the borrower to use a widely accepted risk assessment and management framework, such as NIST SP 800-30. The risk assessment gives borrowers the opportunity to assess the risk associated with each security control, prioritize, and develop a long-term *risk management plan*. It is normal for a risk management plan to address implementation of security controls over a three- to five- year period or more.

Many borrowers are already required to submit documentation of this type to other entities, and they may well be able to provide it to you as well, simplifying your assessment efforts. An additional benefit of requesting and receiving these reports is that they will often include executive or high level summaries that do not require technical expertise to understand.

Assessing Protections and Exposures

If your borrower does not have all three of these components, or if they are a smaller organization with a less mature cybersecurity program, you may want to present them with a smaller subset of questions, some of which may overlap with, or lead to inquiries about, the borrower, which are more in line with traditional diligence concerning a borrower (such as management challenges or over-reliance on key personnel or customers). Consider reviewing the NIST Cybersecurity Framework and similar standards,

©2017 Credit Research Foundation

and choosing questions that are relevant across your population of borrows. Here are a few fundamental topics to include:

- What types of confidential data do you store, and how much?
- How long do you retain sensitive information? What is your process for deleting/disposing of it?
- How do you control access to sensitive information?
- Do you have a formal cybersecurity incident response process?
- How do you conduct user training and awareness?
- Provide copies of contracts with key third-party IT providers (lenders may wish to review the borrower's contracts with vendors and other partners to determine how cyber risks are allocated).
- Have there been previous undisclosed data breaches? If so, please describe.
- Do you have cyber insurance? If so, please provide a copy of the policy for review.

The Intersection of Cyber and "Traditional" Due Diligence

Certain traditional areas of pre-lending inquiry are readily adapted and extended into the realm of privacy and cybersecurity. In particular, questions relating to collateral supporting the loan, as well as liquidation values in the event of default, may have privacy and/or cybersecurity components. Some questions to be considered in this regard include the following:

- Does the borrower have to notify customers or others whose data it holds of the changed financial circumstances or ownership of the organization that may accompany an extension of credit?
- In a secured loan, does the collateral include sensitive data? If so, what restrictions does the borrower (and hence the lender) face in monetizing that data in the event of a default and/or liquidation, and can the lender even foreclose on that data?
- If the lender forecloses on the customer data as an asset, what obligations does that impute on the lender?
- Are there limitations on what the foreclosing entity may do with the customer data once it is obtained?
- Will the lender be required to fund data security maintenance as part of debtor-in-possession (DIP) or other financing?
- Has the borrower adequately maintained the sensitive data, and if not, does the lender need to act to protect it to: (a) avoid a lender liability claim; and/or (b) protect the value of its collateral?

Credit Decisions: Responding to Unsatisfactory Cyber Due Dilligence

Lenders should treat unsatisfactory responses to cyber diligence inquiries as they would any other unsatisfactory information revealed by their underwriting or credit monitoring processes - - they should carefully weigh and consider how a cyber incident may impact the prospective borrower's ability to repay the loan. Said differently, lenders should ask how a cyber incident will affect the borrower's ability to operate. For example, if the borrower is an e-retailer, a cyber attack may render its website outright inoperable, costing lost sales because customers cannot make purchases, or the attack may lead to a customer perception that the borrower is unreliable or unsecure, driving away sales. This reputational and financial damage may be minor, or it can be long-term (as it was for TJ Maxx and Target, which were subjected to years of lawsuits and investigations).

The cyber risks for companies that are not overtly "tech focused" may be more difficult to recognize, but are vital nonetheless. For example, a trucking company may rely on its computer systems to schedule and route deliveries. In the event of a cyber incident, such as a ransomware attack which freezes the company out of that system, the company may be totally unable to operate. Unaffected competitors will undoubtedly pick up the slack, resulting in temporary, if not permanent lost customers.

There is of course, no hard and fast rule for deciding whether or not to lend to a company due to questions regarding its cybersecurity status. At the end of the day, a lender's decision on whether to proceed with a loan to a borrower with unsatisfactory cybersecurity policies, procedures and systems hinges on that lender's general tolerance for risk, and prudent lenders should make cyber diligence a fundamental component of their credit risk evaluation.

Cyber Diligence is a Fundamental Component of Comprehensive Credit Evaluation

Even if cyber diligence does not raise a concern with a potential borrower's cybersecurity status, the simple act of undertaking that evaluation may reveal other credit concerns, such as subtler managerial or operational shortcomings. For example, cyber diligence may reveal that a borrower's supply chain management system is run on antiquated hardware and software that is

©2017 Credit Research Foundation

only understood by one employee - - leaving the company highly vulnerable in the event of the loss or misfeasance of that employee.

It is also important to remember, that just as lenders regularly employ field examiners to check on borrowers' collateral and financial records and controls, lenders should continue to monitor a borrower's cybersecurity status even after a loan is booked and credit is extended. Many borrowers are already required by regulators, vendors or customers to provide annual reports on cybersecurity status for this reason. Just as the borrower's collateral and other financial status may change negatively over time, so too may the borrower's cybersecurity status. For example, if the borrower employed a CISO at the time the loan was booked, but the CISO has since left the borrower and not been replaced, then arguably the borrower is now more vulnerable to cyber incidents than it was at the onset of the loan. This need not be a monumental expense (which in any event would potentially be charged to the borrower in the manner in which field examinations are charged), but can be accomplished through written audits to which the borrower must respond, and/or loan covenants and representations which the borrower must re-affirm at pre-determined times each year.

Conclusion

Lenders to businesses of all sizes and types can benefit from undertaking even a minimal amount of cyber diligence to supplement the traditional diligence and underwriting they undertake when making, extending or modifying a loan. The appropriate level of depth for such diligence will depend upon a number of factors, including the size of the loan, the size, sophistication and industry of the borrower, and ultimately, the lender's appetite for risk.

About the authors:

Erik Weinick *is certified as a Privacy and Cybersecurity Professional (CIPP-US) by the International Association of Privacy Professionals (IAPP) and co-founded the Privacy & Cybersecurity practice group at Otterbourg P.C., which counsels firm clients on privacy and cybersecurity matters. In addition, Erik is a member of the firm's litigation practice group and regularly represents a diverse group of clients, (including many commercial and specialty lenders) before state and federal courts, regulatory authorities, and alternative dispute resolution tribunals.*

Sherri Davidoff *is the CEO of LMG Security and the co-author of "Network Forensics: Tracking Hackers Through Cyberspace" (Prentice Hall, 2012). She has sixteen years of experience as a cybersecurity professional, specializing in digital forensics, penetration testing and security awareness training. She has authored courses for the SANS Institute and Black Hat, and conducted security training for the American Bar Association, Department of Defense, Google, Comcast, Los Alamos National Laboratories and many others. She is also a faculty member at the Pacific Coast Banking School, where she teaches cybersecurity classes.*

Editor's Note: On the next page are some Privacy and Cybersecurity definition of terms and answers to FAQ's related to Cybersecurity

©2017 Credit Research Foundation

Privacy & Cybersecurity: Terms and Concepts to Understand

Big Data – use of data analytics to predict, and even encourage, consumer behavior. Companies which improperly capitalize on PII (defined below) may find themselves the subject of legal action and/or adverse publicity, both of which can impact the company's bottom line.

Chief Information Security Officer or CISO – an officer whose mandate is to maintain the security and integrity of an organization's electronic data. This position is distinct from a Chief Information Officer or Directors of Information Technology, who are tasked with the day-to-day maintenance of an organization's information infrastructure.

Chief Privacy Officer or CPO – an officer whose mandate is to ensure that an organization's use of PII is lawful, appropriate and will not have negative consequences for the organization.

Cybersecurity - focuses on the protection of electronic data and systems so that only authorized users have access.

Privacy – a concept distinct from cybersecurity. This focuses on (i) information privacy (a person's right to keep information about them private) and (ii) communications privacy (the right to privacy in communications).

"Personally Identifiable Information" or "PII" – definitions vary, but generally regarded as a person's name when combined with another identifier, such as a social security number, date of birth, bank account number or other sensitive information, such as health records.

Frequently Asked Questions

What laws or regulations govern cybersecurity? Laws and regulations concerning privacy and cybersecurity can be found at the state and federal level, and may be specific to particular industries, such as recent regulations issued by New York's Department of Financial Services aimed at financial companies and their vendors, or the widely known HIPAA laws governing patient health information and records. Self-regulatory organizations, as well as industry associations, may issue industry-specific regulations and/or guidance.

What are some of the concerns with PII? An organization authorized to receive PII, must first and foremost safeguard that PII, and secondly, must only utilize the PII in the ways authorized by law or contract (which can be inferred from an organization's "promises" to its customers, such as the privacy policies posted to its website).

Will cyber insurance protect an organization from these dangers? While cyber insurance can be valuable, and is highly recommended for organizations of all types and sizes, it is not a panacea. Like all types of insurance, the extent and amount of coverage varies depending upon the policy, and some insurers are more experienced than others when it comes to assisting their policyholders with cyber incidents.

Can an IT director be responsible for privacy and cybersecurity? While IT directors may be well-versed and experienced with privacy and cybersecurity concerns, it is best to have a distinct CISO and CPO, as well as the assistance of outside counsel and cybersecurity consultants for several reasons, including: (i) not all IT professionals, as competent as they may be, are specifically trained in, and sensitive to, privacy and cybersecurity concerns; (ii) IT professionals may have an inherent bias and inability to objectively critique the security vulnerabilities of the very systems they built and/or maintain; and (iii) IT professionals may not have time to adequately focus on cybersecurity as opposed to their primary task of keeping the systems running properly.

©2017 Credit Research Foundation