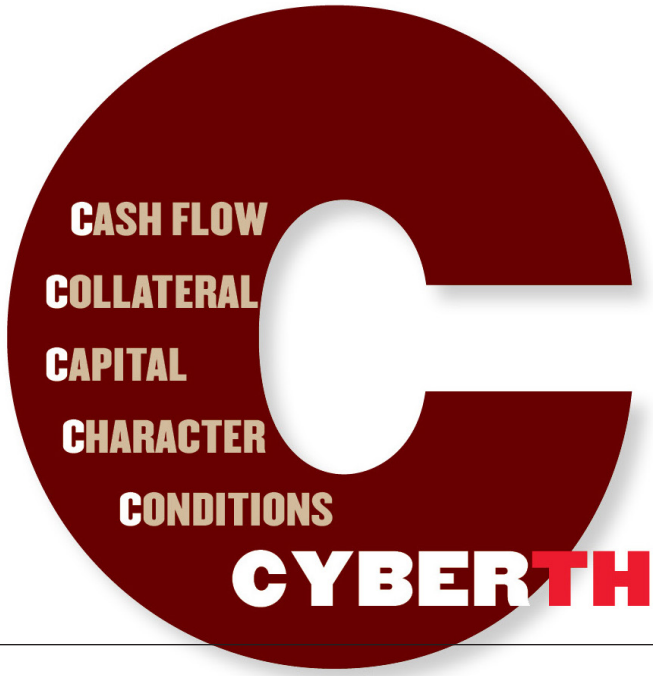
CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW
DECEMBER 2019



THE SIXTH C OF CREDIT IS CYBER

Schoolchildren learn the 3 Rs.
Credit officers learn the 5 Cs.
Now there's a new risk to worry about.

BY KURTIS SUHS

Many of you have heard stories about fraudsters stealing millions of dollars from businesses by compromising their email accounts and using those accounts to initiate fraudulent wire transfers. This story has two sides, though, and today we will discuss how a cyber incident at your customer's business may impact your own organization's cash intake.

I started my career in commercial banking, where I worked as a field examiner in the Asset- Based Lending Group for a major regional bank. One of the primary principles that bankers are taught at the outset of their careers is the 5 Cs of credit. They are cash flow, collateral, capital, character and conditions. These five factors are fairly and evenly balanced by commercial lenders as they assess the risk of lending opportunities.

The banker wants assurance that the corporate borrower (1) will generate enough cash flow to service the debt; (2) has sufficient collateral to cover the loan as a secondary source of repayment; (3) has adequate capital, as banks are more willing to lend to a business whose borrower has an investment in the business; (4) operates in favorable conditions that may impact repayment, including the general state of the economy, industry trends and the use of the loan; and (5) has owners and management of the business who are of sound character—that is, people trusted to honor their commitments. The 5 Cs not only apply in commercial banking, but also to most businesses when they evaluate a credit relationship with a prospective client.

Today, I'm adding a sixth item to the list. Cybersecurity threats have risen to a top concern for many organizations. Ever more sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence have placed the data and assets of corporations, governments and individuals at constant risk. Unfortunately, cyber risk today is mostly treated as an operational risk, which an organization can remediate by purchasing a cyber insurance policy to transfer that risk. However, cyber is much more than an organizational risk. It's also a credit risk, and that's why I label it as the sixth C of credit.

Why Cyber Belongs on the List

Let's examine three examples that help explain why cyber belongs with the other five. A credit rating is a useful tool, not only for the investor but also for entities looking for investors. An investment-grade rating can help a company or a security attract both domestic and foreign investments. Or not.

In May 2019, Moody's lowered Equifax's outlook from stable to negative—the first time that cybersecurity issues had been cited as the reason for a downgrade. Moody's pointed to Equifax's $690 million first-quarter charge for its massive 2017 breach as contributing to the downgrade. The expense represents the company's estimate for settling ongoing class action lawsuits, as well as potential federal and state regulatory fines.

Legal counsel can play an important role in helping senior

management evaluate how a data breach may impact the credit quality of the organization. They can start by identifying the type of personally identifiable information (PII) the company has, the quantity of PII, and its location both inside and outside the organization. The greater the amount of PII, the greater the potential credit impact on the organization. For PII held with third parties, legal counsel should examine the contractual provisions for data protection to ensure that the organization is indemnified and held harmless as a result of a data breach.

For our second example, let's look at a hypothetical. ABC Bank extends an equipment loan to XYZ Company for the cost of computer equipment. But shortly after the purchase, XYZ is hit with a ransomware attack and is left with no means to restore function to the computers. The business files a claim with its insurer for the equipment damage.

Traditionally, the lender would require XYZ Company to name ABC Bank as a loss payee on its property insurance policy. A loss payee is defined as a party to which payment of loss or claim is made before it is directly released to the name insured. The lender, being listed as a loss payee, ensures repayment for their collateral, regardless of potential losses. The loss payee is essentially a safety net for the lender to reduce unpaid loans. If the borrower doesn't list the lender as loss payee, then it's probable that the lender will purchase a "creditor-placed" or "force-placed" insurance policy to protect its collateral—and this new policy is generally far more costly than the client's own policy, so it behooves the client not to let its insurance lapse.

Given that insurers are providing an element of property coverage in cyber insurance, the bank's legal counsel should also advise the banker to require XYZ Company to name ABC Bank as a loss payee on XYZ Company's cyber insurance policy. Many cyber insurers are providing not only the cost to restore, repair and replace hardware as a direct result of a malicious attack, but also the cost to upgrade the insured's hardware, when the upgraded equipment is more secure than the alternative.

In the case of a total loss, the lender will be paid first. If the amount paid out by the insurance company is less than what the borrower owes, then the borrower will be responsible for the remainder. This is where gap insurance comes in handy. If the amount paid by the insurance company is more than what is owed, then the borrower will receive the remainder.

In our third example, let's say that XYZ Company has five clients that represent 35 percent of outstanding accounts receivable. As a result of an insidious and widespread cyber incident, those five companies are unable to repay their accounts receivable in a timely fashion. Ultimately, the majority of those five accounts receivable balances are completely charged off. One way to mitigate this loss is for legal counsel to advise XYZ's credit and risk managers to require that these five clients purchase and maintain cyber insurance. A cyber insurance policy is equally important as a source of financial loss recovery.

The Risk of a Cascade

The common nexus in the above examples is that a credit default has a cascading effect. In a worst-case scenario, a business might not be able to collect its accounts receivable. The business then can't repay its own debt, the bank then writes off the business's commercial loan, and a large portion of the bank's commercial loan portfolio is written off due to that cyberattack that sent shockwaves through its corporate borrowers. The end result is that the bank itself goes under. This, in turn, can threaten the solvency and profitability of the entire banking system, resulting in a general contraction of credit as lenders attempt to protect themselves from losses. Think this can't happen? In 1990 and 1991, 653 banks failed in the United States because of the economic recession and the real estate downturn.

But this doesn't have to happen to banks, companies or the economy. Legal counsel and cyber risk consultants can help create a business strategy that reflects a proactive role in guiding senior management on credit exposures in the portfolio. The basic concept of risk management is to first identify risk. At the micro level, cyber risk can impact an account receivable or a loan. At the macro level, cyber risk can impact a portfolio of accounts receivable or loans.

To have a competitive advantage in today's market, an organization must continue to monitor the credit risk profile of its clients and, at the same time, pursue opportunities to address and minimize cyber risk.

In other words, keep your eyes on that sixth C.

Kurtis Suhs *is the Managing Director of Cyber Special Ops, LLC, (bit.ly/32uL697) a Georgia-based company that he founded to advance cybersecurity by using specialized teams and risk management techniques to prepare for and respond to a cyber event. He has over 33 years of experience in the insurance and financial services sectors, and helped launch the first cyber insurance product in 1997. Using the concierge medicine model, Cyber Special Ops provides guaranteed access to highly credentialed third-party providers for a modest annual membership fee.*