Cybersecurity and Credit Risk

Recent headlines confirm that cybersecurity attacks are an ever-present and growing risk to corporations, financial institutions, governments, and other entities. According to Specops Software research, the U.S. was the most targeted country for cyberattacks between May 2006 and June 2020, followed by the United Kingdom and India.[1] Even corporations and countries in which key economic agents and the government spend a substantial amount of time and resources on comprehensive cybersecurity plans and infrastructure are exposed to significant risks.

Assessing an issuer's management performance and capability has long held a prominent role within Kroll Bond Rating Agency's (KBRA) credit process. In KBRA's view, it is important for an issuer's management team to understand its environmental, social, and governance (ESG) risk profile to mitigate or capitalize on relevant ESG risks and opportunities. KBRA has identified a subset of the most common ESG factors that can be credit-relevant for corporate, financial, and government issuers. These risks include, but are not limited to, stakeholder preferences and reputational risk, climate risk, and cybersecurity risk.

In this report, KBRA focuses on the increased exposure to cybersecurity risk that corporates, financial institutions, and government issuers face, as well as the potential credit implications. Through our research, we have developed potential questions to assess the quality of an issuer's cybersecurity systems, which are included at the end of this report.

Increased Exposure to Cyber Risk

Organizations, regardless of size and industry, are at risk of cyberattacks. According to the Verizon Data Breach Investigations Report (DBIR), most breaches are carried out by external actors and are financially motivated.[2] Fueled by the pandemic and increased reliance on technology, ransomware attacks globally surged 148% in March 2020 compared to baseline levels from February 2020.[3] The losses incurred after a cyberattack are not only monetary—sensitive data and the entity's reputation can also be compromised. Some of the most recent high-profile cyberattacks include the ransomware attack on the Colonial Pipeline, creating severe fuel shortages across the East Coast; data breach of more than 500 million Facebook users worldwide; hackers trying to access Pfizer's data related to the COVID-19 vaccine and treatments; the breach of several federal agencies, known as SolarWinds, that went undetected for months; and the hacking of famous Twitter accounts, including Elon Musk and Bill Gates, for bitcoin.

Cyberattacks targeting health care organizations have also risen in the past year. This is particularly worrisome since criminals can tamper with connected medical devices and potentially jeopardize the patient's life, steal medical records to conduct medical or insurance fraud, or lock down the system in exchange for a ransom. Health care breaches in the U.S. affected over 26 million individuals in 2020.[4] The ransomware attack on Blackbaud, a cloud service provider, was the largest health care breach of the year. Hackers stole customers' fundraising databases and compromised patient and donor information, including medical records, social security numbers, and bank account details. Given the pace and direction of health care's reliance on technology, like the rise in digital health care visits, ultimately all hospitals and health care systems will need to establish strong information technology (IT) systems to effectively operate and successfully protect patient records.

In 2019, there were 104 reported incidences of cyberattacks targeting state and local governments as well as not-for-profit entities, according to cybersecurity firm Recorded Future, with this number likely understated.[5] In a typical municipal-targeted cyberattack, an unknown person or group gains access to a government's computer network, then disables it and seeks a ransom payment to have authorized access restored. Higher profile cases include the city of Baltimore, where many of its systems, including emergency 911 response, was disabled for several days; 22 Texas municipalities that appeared to be subject to a coordinated attack over a brief period; and an attempt to poison the water supply of a Florida town. These and many other troubling examples of cyberattacks disrupt cities, school districts, and other public sector entities. One reason that contributes to this trend is the fact that municipalities, especially smaller ones, have limited resources dedicated to cybersecurity. Further, the essentiality of public services creates vulnerability and the impression

[1] The countries experiencing the most 'significant' cyber-attacks

[2] 2020 DBIR Executive Summary

[3] Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted

[4] Bitglass 2021 Healthcare Breach Report

[5] Recorded Future article dated December 20, 2019: State and Local Government Ransomware Attacks Surpass 100 for 2019.

that there would be a strong motivation to restore normal operations. Paradoxically, the movement toward providing more internet-accessible public services for the many efficiencies and benefits it offers also increases risk.

As more customers rely on digital banking, the number of cyber threats has also grown exponentially within the financial services sector. Financial services firms continue to be the most targeted entities; they are 300x more likely to be attacked than companies in other sectors.[6] Financial institutions that experience a cyberattack may face stakeholder pressures and reputational risk as personally identifiable information of their customers can become compromised. Data breaches can affect a financial institution's ability to operate, potentially causing substantial financial loss. According to a recent paper published by the Federal Reserve Bank of New York, a cyberattack on any of the five largest banks in the wholesale payment network could have severe implications on U.S. financial stability.[7]

Lastly and potentially of most concern, it has become clear that companies across financial services and other major sectors are becoming increasingly interconnected through digital supply chains. This is largely driven by the adoption of cloud services, digital productivity, and collaboration technologies. As a result, threat actors are now adopting more strategic means of attacking large organizations, and larger *groups* of organizations through digital supply chains. The attack on the Texas-based software company, SolarWinds, enabled penetration into some of the most sophisticated and well-defended organizations in the western hemisphere. Victims included Microsoft, multiple U.S. Federal Agencies, and over half a dozen leading cybersecurity product and services firms. Penetration into these organizations enabled cascading impact to their own customers, in which the technologies and services they sell became tainted themselves, and in many cases not only infected their customer bases but disrupted entire businesses operations. For example, Mimecast, a leading email security solutions company, had to notify all of their customers that their integrations with Microsoft had been breached, and then had to forcibly disable email for those customer organizations.[8]

Cybersecurity and Credit Risk

Cybersecurity risks are difficult to quantify. Although the costs and benefits of a good cybersecurity program are sometimes hard to measure, the downside is substantial. In KBRA's opinion, it is important for most public and private sector entities to develop and monitor an effective approach to cybersecurity. KBRA views cybersecurity matters as a key governance issue that reflects management's priorities and can affect an entity's ability to operate. Although limited resources can be a constraint, they do not rule out improvements to cybersecurity programs. Basic improvements to employee training, for example, can provide many benefits and is generally not expensive to implement.

KBRA typically considers an issuer's awareness of and strategy for addressing the many ways cyber risk could impact the organization's operating, financial, and capital strategies and assumptions. Likewise, we often consider management's ability to react to a cyber attack's unanticipated ramifications, such as litigation and/or reputational risk. An effective security response plan that can quickly identify breaches to its internal networks, including those related to foreign threats, provides insight into the quality of monitoring of the risk management team.

Cybersecurity Questions

Analysis of cyber risk management practices can be a critical component of KBRA's assessment of risk management and is often factored into our credit ratings through discussions with management. KBRA has developed a series of questions to help us assess the extent to which an issuer is pursuing best practices in cybersecurity preparedness. We recognize there is no single approach and that the risks will vary across different issuers and will, invariably, change over time. The measures taken to address such risks must also adapt over time. Examples of the cybersecurity questions that KBRA may ask include:

1. Has the entity experienced a cyberattack? What were the ramifications? What was learned from the experience?

2. Does the entity employ a dedicated person/staff to manage information and/or IT security, such as a chief information security officer? *(Someone focused on security is an important indicator of whether the government or issuer takes security seriously.)*

3. Does the entity follow an internationally accepted security standard such as ISO 27001, SSAE-18 SOC reporting, NIST's Cybersecurity Framework, or CIS Top 20 Controls? If so, which ones and is your organization audited to this standard on a regular basis by internal audit and/or third parties? Do you have a set of company policies and procedures to enforce these standards? *(Following a standard and being audited against these criteria are strong indicators whether the entity has a mature security program.)*

[6] Global Wealth 2019: Reigniting Radical Growth
[7] Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis
[8] Important Mimecast Security Update

4. Does the entity have a risk management program? Do they assess their threats and vulnerabilities and determine acceptable risk thresholds? Do they manage risk by prioritizing and structuring their information security program based on the cyber threats most relevant to them? Do they present this to senior management and the board on a regular basis? *(Identifying and prioritizing information security risks is necessary to establish a risk management program. Even more important is regular engagement with the business and senior management so the program is aligned with the business needs, has agreed upon goals, and is staffed with appropriate resources.)*

5. Does the entity have a security awareness program in place and are employees regularly trained and tested on cybersecurity issues? *(Regular security awareness training is important since most security incidents occur due to someone clicking on a link or unwittingly opening an attachment. Employees need to be aware of potential cyber threats, how to detect them, and how not to inadvertently facilitate a cyber breach.)*

6. Does the entity inventory its systems and conduct regular security patches (operating systems and applications)? Are IT and computer systems tested after they are patched (penetration testing and vulnerability scanning)? *(An entity that keeps its systems patched and up to date is less likely to have a security incident. Basic hygiene is important.)*

7. Does the entity run antivirus on all the organization's endpoints and email systems? *(This is a baseline practice. Any entity that is not running antivirus has poor security.)*

8. Does the entity send all appropriate system logs to a security monitoring system and is someone monitoring these logs? *(Ultimately, they will have a security incident, even if minor, and they need the ability to detect it.)*

9. Does the entity have a security incident response plan and is it regularly tested? *(In the event of an IT security incident, it is best practice to follow a preparedness playbook that is calibrated to the type of incident; a set of rules to follow, which have been pre-tested before an actual incident occurs.)*

10. Does the entity have business continuity and disaster recovery plans? Are they regularly tested? *(This question addresses those large-scale incidents that could be very disruptive if they do not have these plans in place and are not tested on a regular basis. The absence of such planning could be a big warning sign.)*

11. Does the entity regularly back its systems to an off-site location and test whether restores are successful? *(Generally, following an incident, systems are required to be restored to a state prior to the incident. The absence of system backups means that the affected entity must start over its IT system from scratch and would likely result in permanent data loss.)*

Conclusion

An effective security program includes a focus on both prevention and remediation should an attack succeed. Cybersecurity is an evolving issue and KBRA will continue to revise and update this list, as necessary. Without proper cybersecurity systems in place, KBRA believes most issuers may be exposed to an increased likelihood of malware and ransomware attacks, and other data breaches, which could lead to negative impact on creditworthiness.

Contacts

Paul Kwiatkoski, Managing Director
+1 (646) 731-2387
paul.kwiatkoski@kbra.com

Andrew Giudici, Senior Managing Director
+1 (646) 731-2372
andrew.giudici@kbra.com

Joe Scott, Senior Managing Director
+1 (646) 731-2438
joe.scott@kbra.com

ESG Contact

Andrea Torres Villanueva, Associate, ESG
+1 (646) 731-1238
andrea.torresvillanueva@kbra.com

Related Reports

Access for free at www.kbra.com

- The Power of the Stakeholder: Oil Majors and Climate Transition Planning
- Financial Institutions: KBRA's Approach to ESG Climate and Reputational Risk Management