MOODY'S INVESTORS SERVICE

SECTOR IN-DEPTH
22 January 2020

Rate this Research

TABLE OF CONTENTS

Analyst Contacts

Leroy Terrelonge 1.212.553.2816
AVP-Cyber Risk Analyst
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
Vice President – Senior Analyst
lesley.ritter@moodys.com

Gerald Granovsky +1.212.553.4198
Senior Vice President
gerald.granovsky@moodys.com

Michael Rowan +1.212.553.4465
MD-Gbl Pub Proj and Infra Fin
michaelj.rowan@moodys.com

Jim Hempstead +1.212.553.4318
MD-Utilities
james.hempstead@moodys.com

Cyber Risk – Global

Digitization and attack sophistication will pose heightened cyber risks in 2020

Summary

» **Cyber risks are rising, with potential credit implications for an array of sectors.** Growing use of digital technologies in business operations and cyberattack sophistication pose increased business disruption risk and put more sensitive data at risk of disclosure.

» **Ransomware attacks will become more targeted.** Ransomware attacks will continue their evolution from diffuse, opportunistic attacks to targeted attacks that increasingly involve theft and public disclosure of data.

» **Cloud misconfigurations will result in more data breaches.** More organizations will adopt cloud services for scale and efficiency, but human error in setting up these services will continue to lead to data breaches.

» **Data privacy regulations will lead to higher and more frequent fines.** Although fines alone have not yet threatened companies' credit quality, the upward trend in fine amounts points to a need for robust liquidity reserves or other alternate sources of liquidity to absorb any adverse penalties in 2020.

» **Political and geopolitical cybersecurity concerns pose growing risks.** Government-sponsored cyberattacks against adversaries will continue, while fears of cyber meddling in the 2020 US presidential election persist.

» **Supply chain concerns will rise.** Supply chain concerns will lead to continued geopolitical disputes, exposing technology companies operating in adversarial nations to increased scrutiny, investigations and bans. Additionally, as downstream organizations harden their cyber defenses, vendors and software providers further upstream will remain risks in the supply chain.

» **Artificial intelligence (AI)-based cyberattacks will mature.** AI knowledge and tools are becoming more accessible, which will result in more attacks that leverage AI techniques. Organizations will need to adapt their defenses in response.

» **Cyber insurance litigation will spread.** Confusion about cyber insurance policies and what they cover will lead to increased litigation.

» **Companies will work to better protect operational technology (OT) networks.** The exposure associated with cyber risks and industrial processes will become a bigger priority for managers of organizations.

Cyber risks are rising, with potential credit implications for an array of sectors

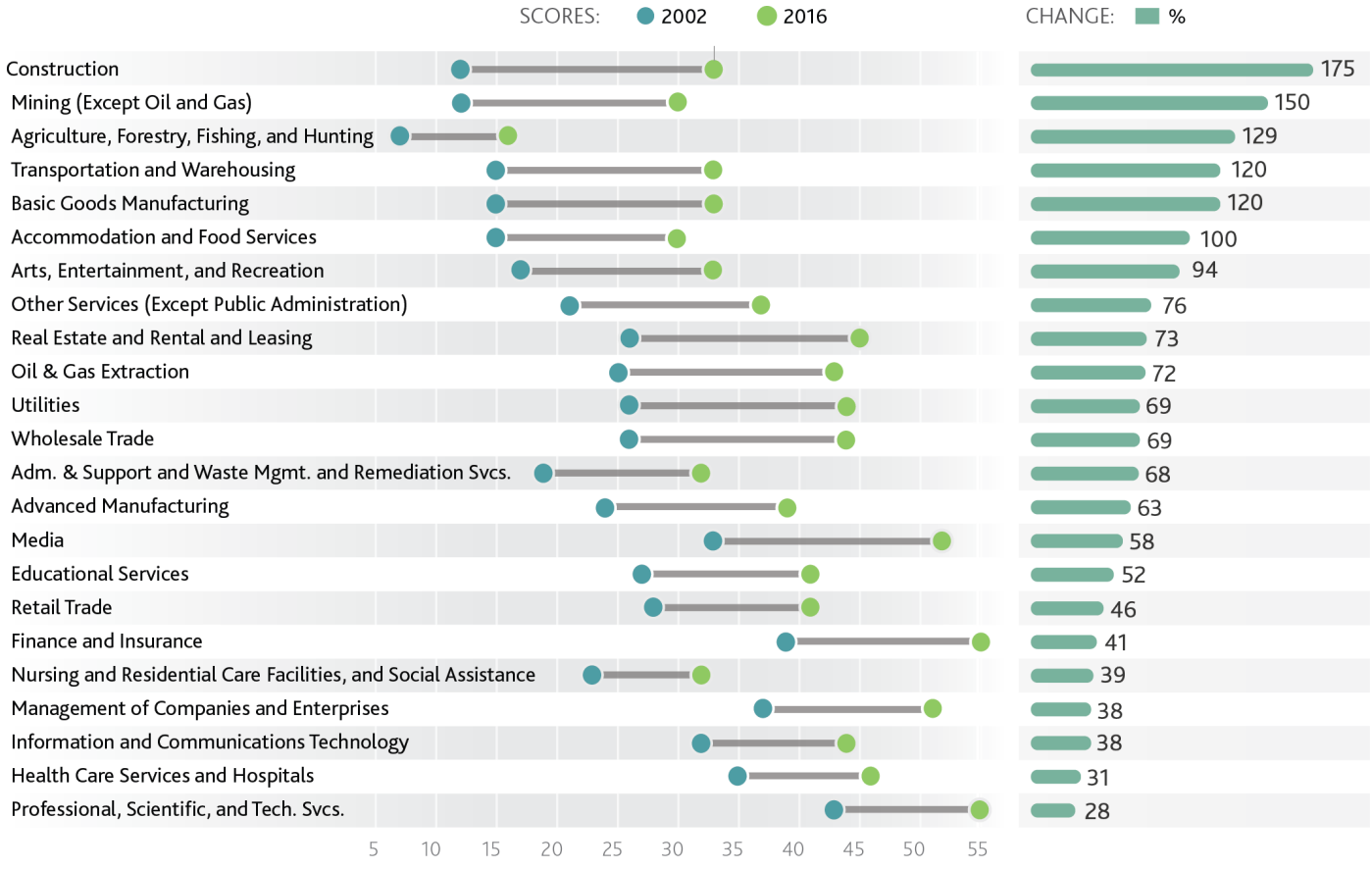
Cyber events have the potential to create bigger credit implications in 2020 than in the past owing to ever-increasing risks. Data from the FBI's Internet Crime Complaint Center point to the growth and intensity of cyber events, with reported cyber incidents worldwide rising 31% and losses from cybercrime increasing 238%, from $800 million to $2.7 billion, between 2014 and 2018.[1]

Cyber incidents have had credit-negative implications for many issuers by affecting their financial profiles, reducing liquidity, increasing exposure to litigation or hurting corporate reputations. These incidents also increase risk for boards of directors, trustees or other executives with accountability. To date, however, we have only taken one rating action as a direct result of the forward credit implications of a cyber incident. This occurred in May 2019 when we lowered the outlook of Equifax Inc. (Baa1 negative) to negative from stable.[2]

The growing reliance on digital technologies in business operations is a key reason for the rising risks. Research from the Brookings Institution shows that digitization rose in 517 of 545 analyzed occupations between 2002 and 2016, with the average digitization score up 57% (see Exhibit 1). Sectors with the most rapid digitization growth included construction, mining, agriculture, transportation and manufacturing.[3]

Exhibit 1

Sector mean digitization scores and percent change, 2002 and 2016



Sources: The Brookings Institution and Moody's Investors Service

At the same time, the sophistication of attacks is increasing because highly sophisticated tools developed by nation-states are falling into the hands of less-skilled attackers as a result of data breaches. Examples include tools leaked in separate incidents between 2016 and 2019 from the US National Security Agency (NSA) and Central Intelligence Agency, as well as from the Iranian Ministry of Intelligence. One of the NSA tools, code-named ETERNALBLUE, was incorporated into the WannaCry and NotPetya cyberattacks of 2017 that infected tens of thousands of computers around the world.[4]

With the availability of advanced cyber tools, attackers themselves do not need to possess a high degree of sophistication to launch sophisticated attacks. In fact, the average level of sophistication among cyberattackers has decreased precipitously, even as attacks have become more advanced.[5]

Ransomware attacks will become more targeted

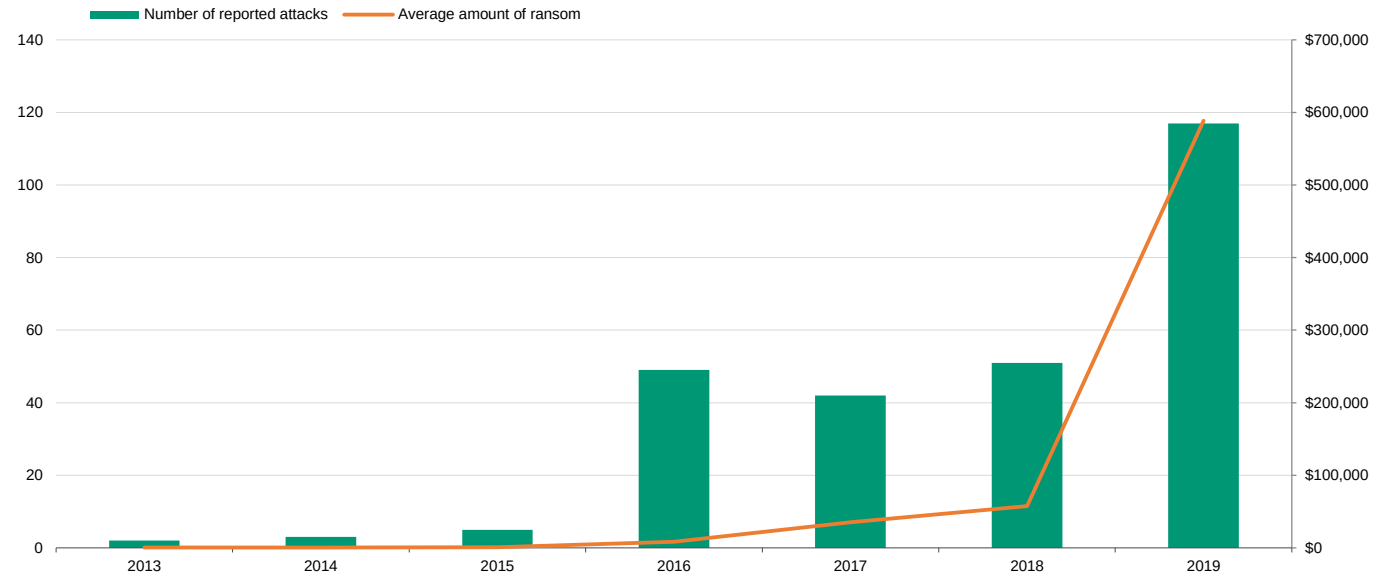
Targeted ransomware attacks, in which attackers block access to victims' data or computer systems in exchange for a ransom payment, picked up speed in 2019 and will continue to gain pace in 2020. In prior years, ransomware attacks had been opportunistic, often distributed at random to individual computer users with ransom amounts in the low hundreds of dollars. But more recently, attackers have also stolen data that they then threaten to release publicly if they are not paid. Release of sensitive data adds reputational and data breach concerns for victims, as well as creating risk of losing intellectual property.

Targeted ransomware attacks have hit regional and local governments (RLGs) particularly hard (see Exhibit 2). Private entities may be able to hide the effects of a ransomware attack from the public, but it is clear when an RLG can no longer provide services to its constituents. While 70% of victim RLGs assert that they have not paid the ransom, cybercriminals are profiting significantly from the victims that do pay, making it likely that RLGs will remain targets in 2020.[6]

Exhibit 2

The number of ransomware attacks and ransom amounts soared in 2019

Ransomware attacks against US regional and local governments, 2013 to 2019



Sources: StateScoop and Moody's Investors Service

Hospitals and health service providers around the world will also continue to be a visible target of ransomware attacks. These facilities are attractive targets because they hold valuable data such as personal health information and payment card data, and they typically lack the resources for dedicated cybersecurity personnel and tools.[7] Additionally, healthcare facilities have high incentives to pay ransoms because ransomware disruptions can jeopardize patient safety by delaying or preventing the provision of care. Some small healthcare facilities have closed down permanently because of the costs of recovering from ransomware attacks.[8]

Managed services providers (MSPs) will remain key ransomware targets

MSPs will also remain highly attractive ransomware targets, given that attacks against them are lucrative and targets are plentiful. MSPs most often operate as IT providers for small and medium-size entities (SMEs). SMEs generally find it cheaper and more efficient to use MSPs than to build and maintain their own IT functions.

However, because MSPs store and process data for dozens of customers, attackers can paralyze many entities through an attack on one organization. For example, in August 2019, 22 towns in Texas (Aaa stable) simultaneously fell victim to a ransomware attack on TSM Consulting Services Inc., an MSP.[9] The attacker demanded $2.5 million, well above the typical $400,000 to $600,000 demanded of municipalities.[10] Texas state officials responded to the attack by activating a task force consisting of cybersecurity experts from academia, the military, and government. With the task force's support, the towns restored operations without paying any portion of the ransom.[11]

Ransomware attackers will turn to data theft to increase likelihood of payment

The calculus for victim organizations in deciding whether or not to pay a ransomware demand will change with the rise of attackers who steal data before locking victims' access to it. As more organizations implement effective backup procedures that allow them to ignore ransom demands, attackers will seek additional pressure points to coerce victims into paying.

For example, in late 2019, ransomware gang Maze began to steal data and pressured victims to pay by threatening to publicly identify them and distribute their sensitive data if they did not meet the ransom demands.[12] In one such instance, Allied Universal (B3 stable), a security staffing firm, experienced a ransomware infection in November 2019. When the company did not pay a ransom by the deadline, the attackers released almost 700 MB of sensitive employee and business information.[13]

Most companies have no obligation to report ransomware attacks except under specific circumstances, but under data privacy laws, companies in many jurisdictions must report unauthorized access to customer data. They also may face hefty fines for not safeguarding data. This is an especially acute issue for the US healthcare sector, as the Health Insurance Portability and Accountability Act prescribes fines of up to $50,000 per violation, with a maximum penalty of $1.5 million per year per violation type.[14]

Transparency push from public and investors will ratchet up

More companies will adjust their communications strategies to provide information earlier in the response process to a ransomware attack as a result of increased pressure for transparency from the public and investors.

For example, Norwegian aluminum and renewable energy company Norsk Hydro's (Baa2 negative) response to a ransomware attack in March 2019 showed that not only was it possible for a company to proactively provide information on disruptive cyber incidents, but that investors will reward a company for its transparency. Norsk Hydro set up a website to disseminate factual information on the ransomware attack, drafted social media posts to detail progress on recovery efforts, and held daily webcasts with senior staff answering questions from a virtual audience.

While few companies have matched Norsk Hydro's level of transparency, some have decided to proactively announce when they have fallen victim to cyber incidents that disrupt production. For example, Pitney Bowes (Ba2 stable) announced in October 2019 that it had experienced a malware attack that encrypted information on some of its systems and disrupted customer access to certain services.[15]

Cloud misconfigurations will result in more data breaches

Data breaches caused by cloud misconfigurations will likely grow in 2020 as a result of the increasing adoption of cloud technology, the complexities of cloud computing and the relatively small number of cloud security experts. Cloud misconfigurations often result from an incorrect implementation of security and access protocols.

Overall, cloud migration tends to result in better cybersecurity. This is especially true for SMEs that benefit from the large security budgets and specialized security personnel of cloud providers such as Amazon (A3 positive), Microsoft (Aaa stable), and Google, a subsidiary of Alphabet Inc. (Aa2 stable) However, cloud implementation can introduce human error that causes data to be exposed. For example, cybersecurity vendor Imperva (B3 stable) announced in August 2019 that attackers had accessed a copy of a company database to steal emails, cryptographically protected passwords, application programming interface keys, and transport layer security

keys from subsets of Imperva Cloud Web Application Firewall customers.[16] The attacker gained access to the sensitive database copy because a misconfiguration left a key server publicly accessible.

Cloud providers have introduced security improvements to reduce misconfigurations, including brightly colored warnings that appear on the screen when users' data is publicly accessible and easier-to-use controls for restricting access to data. Customers, however, continue to struggle with improper implementation of cloud security controls.

Data privacy regulations will lead to higher and more frequent fines

The introduction of data privacy laws in a number of large jurisdictions raises the likelihood of more frequent and higher fines in 2020.

In 2019, regulators imposed record fines for data privacy issues. For example, in July 2019, the UK's Information Commissioner's Office (ICO) announced its intention to fine British Airways PLC (Baa3 positive) $230 million for a data breach the company announced in September 2018. The breach resulted in the theft of login credentials, payment card data, travel booking details and associated names and addresses for roughly 500,000 of the airline's customers.[17] Also in July 2019, the ICO announced its intent to issue a $125 million fine against Marriott International, Inc. (Baa2 stable) related to a security incident involving the Starwood guest reservation database that the company disclosed in November 2018. That incident involved up to 383 million customer records.[18]

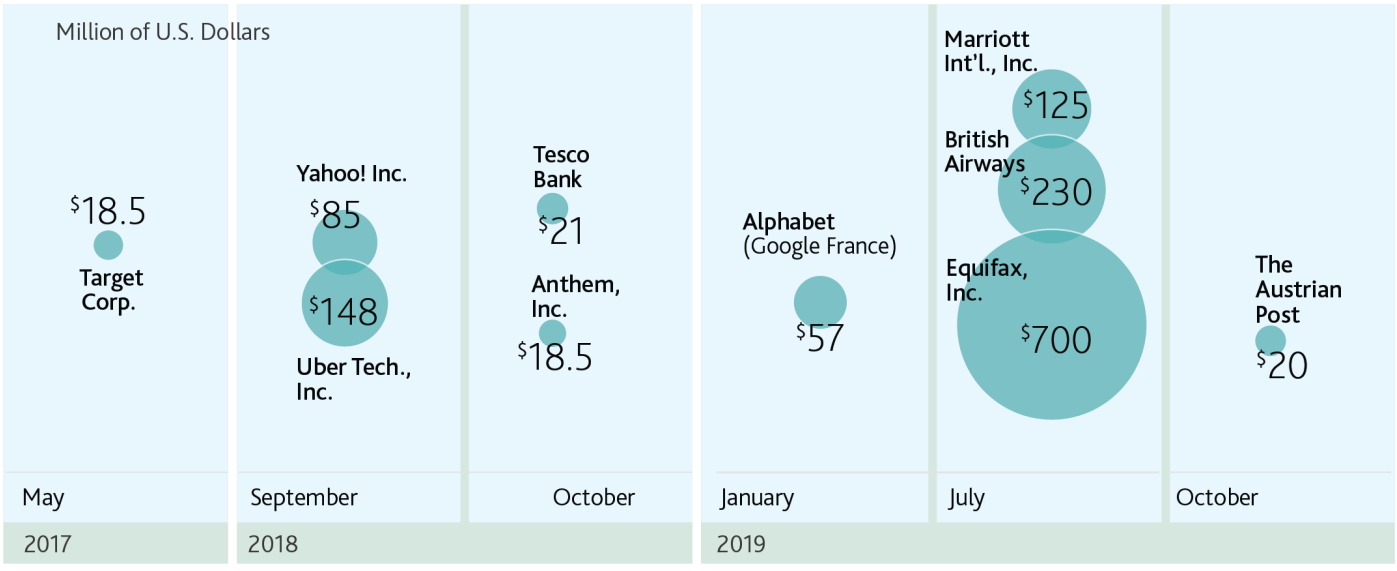
These fines represented record amounts under Europe's General Data Privacy Regulation (GDPR) that went into effect in May 2018, and are harbingers of higher and more frequent fines under additional data privacy regulations. Among GDPR fines, only one fine in 2018 exceeded $100,000, whereas there were 27 above that level in 2019. Furthermore, all of the six fines above $1 million in 2019 occurred in the second half of the year, pointing to the upward trend in fine amounts.[19]

While the proposed fines against British Airways and Marriott rank among the top five largest data breach fines globally, they fall far short of the up to $700 million Equifax agreed to pay as part of a settlement announced in July 2019 (see Exhibit 3).[20]

Exhibit 3

Top 10 data breach fines and settlements globally

Fines and settlement amounts continue to grow over time



Date listed is the month the fine or settlement was announced.

Source: Moody's Investors Service

In the US, the California Consumer Privacy Act took effect on January 1, 2020, and will further contribute to the higher tempo and increased dollar amounts of data breach fines. Although the law applies only to businesses operating in California, the state's heft in the US economy and its concentration of internet technology giants make it likely that many large companies around the US will extend the law's protections to all US customers, as Microsoft Corp. (Aaa stable) has pledged to do.[21]

Meanwhile, Indian legislators introduced a bill that will constrain how companies process individuals' data and establish a new entity known as the Data Protection Authority to enforce the law's provisions. Set in motion following a landmark 2017 Indian Supreme Court decision that declared a constitutional right to privacy, the bill would provide privacy safeguards for the 1.3 billion people that make up the world's second most populous country.[22]

Political and geopolitical cybersecurity concerns pose growing risks

Governments use cyberattacks to achieve geopolitical goals, and these cyberattacks can target rated entities directly, or rated entities can become collateral damage in attacks that may not have intended to target them.

An example of direct targeting of rated entities occurred in 2011 to 2013 when Iranian government contractors launched distributed denial-of-service (DDoS) attacks against 46 victims, primarily in the US financial sector.[23] The attacks prevented clients from accessing these institutions' websites, and US intelligence officials reportedly believed they were retaliation for US-imposed economic sanctions to counter Iran's nuclear program.[24] In an example of indirect targeting, Russia's military intelligence directorate reportedly launched the NotPetya ransomware attack to target Ukraine, but the ransomware ultimately infected tens of thousands of computers around the world and disrupted business operations for multiple large companies.[25]

This year began with security warnings from the US Federal Bureau of Investigation and the Department of Homeland Security about the risk of potential cyberattacks from Iranian or Iran-supported attackers in the wake of rising tensions with the US. Although it is difficult to predict which sectors would be most at risk, there would likely be a wide range of potential targets across multiple geographic regions. Credit impact of a successful cyberattack would depend on the scale, scope and duration of the event.[26]

Additionally, cyber meddling remains a concern for the US presidential election slated for November 2020. But while there have been many reported cases of cyberattacks related to elections, including in the US (Aaa stable), France (Aa2 positive), Germany (Aaa stable), Hong Kong (Aa3 stable), Israel (A1 positive) and throughout the Commonwealth of Independent States (CIS), these episodes have not had an impact on a government's creditworthiness. Thus far, despite multiple reported cases, it has been very difficult to prove with absolute certainty that a cyberattack occurred and resulted in material election interference. Meanwhile, clearly determining the ultimate impact on final election results is highly challenging. Nonetheless, if there were a successful cyberattack that was indeed proven with certainty and that resulted in clear interference with final election results, it could have credit implications, especially if the outcome were to lead to a clear shift toward more credit-negative policy developments.[27]

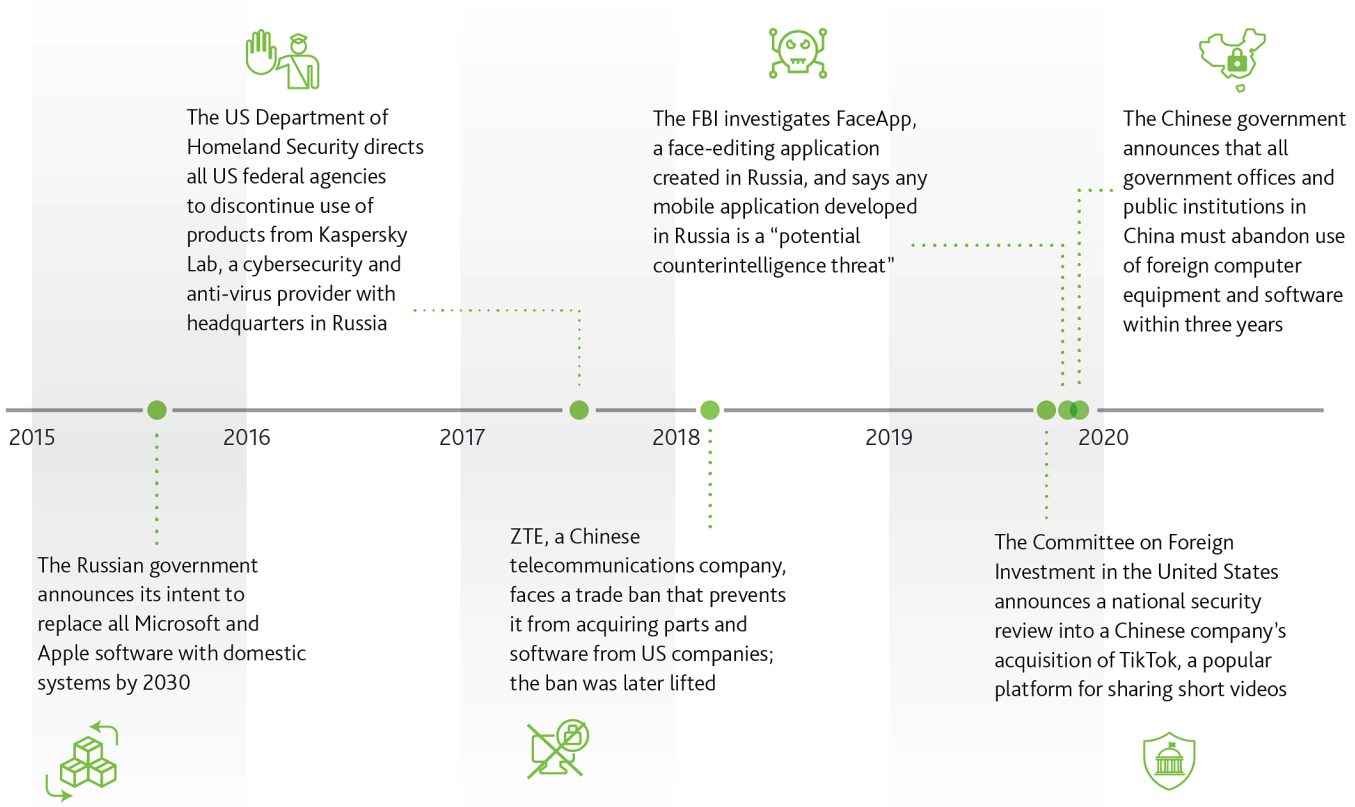
Focus on national security supply chain concerns will rise

Some governments will likely take further punitive actions against foreign technology companies in 2020, citing national security concerns. As a result, technology companies will likely find themselves locked out of lucrative government contracts in adversarial countries, or even banned completely, with resulting downward pressure on their revenue.

Governments fear that these companies may use their access to sensitive domestic computer and telecommunications systems to engage in espionage or sabotage (see Exhibit 4). For example, starting in February 2020, US companies will be banned from selling hardware, software or other products to Chinese technology giant Huawei without a license. In response to the ban, which the Trump administration planned for 2019 but later postponed, Huawei CEO Ren Zhengfei slashed Huawei's 2019 revenue expectations to $100 billion from $130 billion.[28] However, the revenue impact was muted owing to the ban's postponement, and Huawei announced a record $122 billion in revenue for 2019.[29]

Exhibit 4

Foreign technology companies are increasingly coming under scrutiny from government authorities



Sources: The Moscow Times, Reuters, The New York Times and Financial Times

Risks from vendors and software supply chain exposure will continue

As organizations employ more effective security measures and become harder targets to compromise, determined attackers will increasingly turn to other entities that have privileged access to targeted networks: vendors and software providers.

Vendors

Attackers will target organizations through vulnerable vendors. Vendors gather, store, and process data on behalf of organizations, and in some cases have direct access to the organization's computer network. They are, however, often smaller, have fewer resources, and are less able to secure their own operations than the organizations they work for, which attackers can exploit.

In June 2019, American Medical Collection Agency, a billing collections vendor, announced a data breach that potentially exposed personal information for millions of healthcare customers. The breach affected the two largest clinical laboratories in the US, Quest Diagnostics Inc. (Baa2 stable) and Laboratory Corporation of America (LabCorp, Baa2 stable), exposing data for 11.9 million and 7.7 million of their customers, respectively. Similarly, data breaches in 2017 and 2019 that affected certain cities in the US and Canada underscored the cyber risks for RLGs related to commercial vendor relationships. In these incidents, attackers stole payment card data, locally hosted and managed on the cities' computer systems, for residents who had used billing software Click2Gov from CentralSquare Technologies, LLC (Caa1 negative).[30]

In an example of industrial espionage, malicious actors reportedly attempted to steal intellectual property and defense secrets held at Airbus (A2 stable) by targeting four of the company's suppliers: Rolls-Royce plc (Baa2 stable), French engineering, quality services and management consulting company Expleo, and two additional unnamed suppliers.[31]

Software supply chain

Vulnerabilities in the software supply chain will continue to attract attackers given that software can grant them access to victims' computer networks. For example, in March 2019, researchers at Kaspersky Lab reported that unidentified attackers had compromised servers at Taiwan-based computer hardware company ASUS, hijacking the company's automatic software update service to install so-called backdoors (malware that provides persistent access to compromised devices) on half a million ASUS computers.[32]

In another incident, researchers in August 2019 published a suite of vulnerabilities present in hundreds of millions of devices around the world, primarily industrial controls systems, Internet of Things devices, medical devices, routers and security cameras.[33] Many device owners did not know they were affected, even though the vulnerabilities were widely publicized, because they had little visibility into the software components of the supply chain.

In response to these challenges, the US National Telecommunication and Information Administration has been promoting the concept of a software bill of materials (BOM).[34] In the same way a bill of materials is a comprehensive inventory of the raw materials, parts, components and quantities of each needed to manufacture of product, a software BOM is a list of the ingredients that make up software components and provides visibility that enables organizations to monitor known vulnerabilities or unsupported software. Software BOM promotion efforts will continue in 2020.

AI-based cyberattacks will mature

The pace of technological advancement continues to democratize access to AI technology. Although cyberattacks involving known use of AI so far remain uncommon, they will likely increase in 2020.

Recent attacks, including both real-world attacks by malicious actors and simulated ones by security researchers, underscore the rising AI risks. In March 2019, fraudsters reportedly used AI-based software to create a deepfake imitation of a chief executive's voice that was used to trick a subordinate at a UK-based energy firm into transferring $243,000 to a bank account in Hungary.[35] The incident is the first publicly known cybercrime attributed to this AI technique, which relies on deep learning to create fake content.

Researchers have shown that it is relatively easy to trick AI systems and defeat their original purposes. In one instance, researchers fooled an anti-virus platform into categorizing known malware as harmless.[36] In another case, researchers at the University of California, Berkeley, showed that attackers could construct and issue audio commands to AI virtual assistants, such as Apple's Siri or Amazon's Alexa, that are undetectable to the human ear.[37] Attackers hid the commands in white noise or in music, and could use them to unlock doors, wire money, or buy items online. Researchers in Japan achieved similar control of AI assistants by shining laser pointers or flashlights at them from hundreds of feet away.[38]

If researchers can find these flaws, it stands to reason that malicious actors can too, and as more and more processes and devices are connected to AI systems, the attack surface for adversarial AI attacks will increase commensurately.

Cyber insurance litigation will spread

Demand for cyber insurance will increase in 2020, driven by the intensification of cyberattacks and the associated costs, the heightened focus by boards of directors and risk managers, and recent regulations. At the same time, litigation will spread as organizations and insurance companies differ in their interpretations of the coverage offered.

For example, two closely-watched legal cases are addressing the issue of whether the war exclusion in most traditional property and casualty (P&C) policies applies to cyberattacks. After the 2017 NotPetya malware attack damaged tens of thousands of computers around the globe, some corporations filed claims under cyber coverage embedded in traditional P&C policies. Certain insurers, however, denied coverage under P&C policies, arguing that the attack was an act of war because the US, the UK and several other countries had attributed it to the Russian government and its efforts to destabilize Ukraine; P&C insurance policies generally exclude coverage for acts of war.[39]

Two of the companies denied coverage, Merck & Co., Inc. (A1 stable) and Mondelez International, Inc. (Baa1 stable), filed lawsuits in 2018 against their respective insurers seeking damage under all-risk property policies. The insurance industry is closely monitoring the courts' interpretations of the specific language in the individual contracts because they will help clarify the scope of cyber coverage

within traditional policies. These cases also demonstrate that collecting on claims can be a lengthy process depending on complexity of the claim, specific policy wording and coverage triggers.

Confusion over insurance coverage could also accompany an extension of the US Terrorism Risk Insurance Program Reauthorization Act (TRIPRA). The act, which expires in December 2020, provides businesses with a government reinsurance backstop in the event of a large-scale terrorist attack. In 2016, the US Department of the Treasury clarified that the program covers acts of cyberterrorism.[40] Some cyber activity, however, defies easy categorization and raises questions about coverage under this act. For example, as a state actor, an Iran-directed cyberattack could be labeled as an "act of war," which is an exclusion under TRIPRA. But Iran also financially supports organizations on the US government's foreign terrorist organization list, so an attack by Iran through its proxies could be labeled as terrorism, and thus covered under TRIPRA. If lawmakers renew the act, they have said they will study and make recommendations for the cyberterrorism coverage program, which would help resolve potential coverage misunderstandings.[41]

Companies will better protect OT networks

Businesses will likely become more aware of their OT risk exposure in 2020, and as a result, security offerings will evolve and organizations will be better prepared to prevent, detect and recover from cyber incidents. OT networks have less mature cybersecurity practices that trail those of information technology (IT) networks. Physical assets operating in the OT environment only recently began to adopt digital technology in a significant way.

According to an October 2015 report from The Center for Strategic and International Studies, the defenses around OT are a full decade behind the current levels of defenses for information technology.[42] OT assets were set up to operate on a standalone basis, in a siloed environment and over multiple decades, with the primary goal of achieving the highest levels of availability and reliability. This contrasts with IT assets, which have long been networked and have operational lives of less than a decade.

Increased awareness of OT vulnerabilities is assisting in the maturation process of securing OT networks. In 2019, a number of reported cyberattacks impaired operational processes. Attackers deployed ransomware against the automotive activities of Germany's Rheinmetall AG (Baa3 stable), disrupting operations in September at three Rheinmetall Automotive plants in the Americas (the US, Mexico, and Brazil). This attack was reminiscent of the March ransomware attack on Norsk Hydro[43] and the June ransomware attack on Belgian aviation equipment maker ASCO, which also affected industrial processes.[44]

In the utilities sector, researchers found malware in the IT network of the Nuclear Power Corporation of India Limited's Kudankulam nuclear power plant in October 2019, which may have presaged an attempt to compromise the OT network.[45] And a campaign targeting US utilities located close to dams, locks, and other critical infrastructure came to light in November.[46]

Moody's related publications

Sector research

- Credit implications of cyber risk will hinge on business disruptions, reputational effects, February 2019
- Battling hidden cyber exposures, insurers position for growing opportunity, July 2019
- Deepfake disinformation campaigns pose reputational risks to businesses, August 2019
- Cyberattacks pose growing operational and financial risks for hospitals, September 2019
- Local government – US: Ransomware attacks highlight importance of IT investment and response planning, October 2019
- Cyber Risk – Global Investment Banks: GIBs heighten readiness against constant cyber threat, October 2019
- Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, October 2019
- Cyber Risk – Global: Cyberattacks on governments are rising but pose limited risks to credit quality, November 2019
- Regulated utilities and power companies - North America: Grid modernization heightens vulnerability of utilities to cyberattacks, November 2019
- Infrastructure & Project Finance – Global: Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure, November 2019
- Sovereigns - Global: Digital technologies likely to enhance credit profiles for countries that leverage benefits while managing disruptions, November 2019
- US-Iran tensions raise cyber risk; credit impact would depend on attack severity, January 2020

Issuer research

- Matanuska-Susitna (Borough of) AK: Quick, coordinated response, access to emergency funds and insurance limit cyberattack losses, March 2019
- Severe cyberattack forces operations into partial manual mode, a credit negative, March 2019
- Baltimore (City of) MD Second ransomware attack in 15 months disrupts Baltimore's operations, May 2019
- Equifax Inc.: Cybersecurity investments, lagging operating performance and debt-funded M&A to weigh on metrics, May 2019
- Data breach at Quest and Lab Corp highlights cyber risk in vendor relationships, June 2019
- City of Johannesburg (South Africa): Response policy mitigates impact of cyberattack, July 2019
- Marriott announces the UK Information Commissioner's Office's intent to issue fine related to Starwood breach, July 2019
- British Airways faces record-breaking data privacy fine, a credit negative, July 2019
- Pitney Bowes Inc. malware attack is credit negative but no immediate impact to ratings, October 2019

Topic page

- Cyber Risk

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

Endnotes

1 FBI 2018 Internet Crime Report, Internet Crime Complaint Center, April 22, 2019.
2 Equifax Inc.: Cybersecurity investments, lagging operating performance and debt-funded M&A to weigh on metrics, May 22, 2019.
3 Digitalization and the American Workforce, Metropolitan Policy Program at Brookings, November 2017.
4 WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017, Alex Hern, The Guardian, December 30, 2017
5 Vulnerability Discovery: Bridging the Gap Between Analysis and Engineering, Computer Emergency Response Team, Carnegie Mellon University, 2006.
6 Early Findings: Review of State and Local Government Ransomware Attacks, Recorded Future, May 10, 2019.
7 Cyberattacks pose growing operational and financial risks for hospitals, September 12, 2019.
8 Smaller Medical Providers Get Burned by Ransomware, Adam Janofsky, The Wall Street Journal, October 6, 2019.
9 The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once, ProPublica, September 12, 2019.
10 22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault, Bobby Allyn, NPR, August 20, 2019.
11 Update on Texas Local Government Ransomware Attack, Texas Department of Information Resources, September 5, 2019.
12 Another ransomware strain is now stealing data before encrypting it, ZDNet, December 18, 2019.
13 Allied Universal Breached by Maze Ransomware, Stolen Data Leaked, BleepingComputer, November 21, 2019.
14 Federal Register, Volume 78 Number 17, Department of Health and Human Services, p. 5582, January 25, 2013.
15 Pitney Bowes Inc. malware attack is credit negative but no immediate impact to ratings, October 15, 2019.
16 Imperva security incident is credit negative but no impact on credit profile at this time, September 1, 2019.
17 British Airways faces record-breaking data privacy fine, a credit negative, July 11, 2019.
18 Marriott announces the UK Information Commissioner's Office's intent to issue fine related to Starwood breach, July 9, 2019.
19 Major GDPR Fine Tracker, Alpin, December 17, 2019.
20 Equifax to Pay Up to $700 Million in Data Breach Settlement, Dave Sebastian and AnnaMaria Andriotis, The Wall Street Journal, July 22, 2019.
21 Microsoft will honor California's new privacy rights throughout the United States, November 11, 2019.
22 On Data Privacy, India Charts Its Own Path, The New York Times, December 10, 2019.
23 Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector, US Department of Justice, March 24, 2016.
24 Denial of service attacks against U.S. banks in 2012–2013, Cyber Operations Tracker, Council on Foreign Relations.
25 The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Andy Greenberg, Wired, August 22, 2018.
26 US-Iran tensions raise cyber risk; credit impact would depend on attack severity, January 2020.
27 Cyberattacks on governments are rising but pose limited risks to credit quality, November 2019.
28 Huawei says U.S. ban hurting more than expected, to wipe $30 billion off revenue, Sijia Jiang, Reuters, June 17, 2019.
29 Huawei's Revenue Hits Record $122 Billion in 2019 Despite U.S. Campaign, The Wall Street Journal, December 30, 2019.
30 Second Wave Of Click2Gov Attacks Hits Billing Systems In 8 Cities, Forbes, September 22, 2019.
31 Hackers target Airbus suppliers in quest for commercial secrets, AFP News, September 26, 2019.
32 Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers, Vice Motherboard, March 25, 2019.
33 Decades-Old Code Is Putting Millions of Critical Devices at Risk, Wired, October 1, 2019.
34 NTIA Software Component Transparency, National Telecommunications and Information Administration (US Department of Commerce), December 2019.
35 Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, Catherine Stupp, The Wall Street Journal, August 30, 2019.
36 Researchers Easily Trick Cylance's AI-Based Antivirus Into Thinking Malware Is 'Goodware', Vice Motherboard, July 18, 2019.
37 Alexa and Siri Can Hear This Hidden Command. You Can't, The New York Times, May 10, 2018.
38 With a Laser, Researchers Say They Can Hack Alexa, Google Home or Siri, Nicole Perlroth, The New York Times, November 4, 2019.
39 Battling hidden cyber exposures, insurers position for growing opportunity, July 2019.
40 Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program, US Department of the Treasury, December 27, 2016.
41 House passes terrorism backstop extension, Business Insurance, November 19, 2019.
42 The Case for Simplicity in Energy Infrastructure, Center for Strategic International Studies, October 30, 2015.
43 Severe cyberattack forces operations into partial manual mode, a credit negative, March 21, 2019.
44 Asco closure after cyber-attack to last another week, Alan Hope, The Brussels Times, June 22, 2019.

45 Cyberattack on Indian nuclear plant shows vulnerabilities of critical infrastructure, November 8, 2019.
46 Utilities Targeted in Cyberattacks Identified, Wall Street Journal, November 24, 2019.

REPORT NUMBER 1206292

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE