MOODY'S INVESTORS SERVICE

SPECIAL SERIES Credit After Covid

SECTOR IN-DEPTH
8 July 2020

Rate this Research

Contacts

Alessandro Roccati +44.20.7772.1603
Senior Vice President
alessandro.roccati@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

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

CLIENT SERVICES

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

Financial Institutions – Cross Region

Cyber risk rises as coronavirus drives increased digital banking and remote work

The coronavirus outbreak is accelerating an existing shift to digital banking and remote work that exposes banks to greater risk of cyberattacks, primarily motivated by financial gain. This broad change in consumer and work habits will not only entail significant changes to bank business models[1] but also require banks to maintain a high level of cyber risk awareness and take mitigating actions to curtail the additional risk.

» **Large-scale shift to digital banking and remote work has accelerated the technology cycle and increased banks' vulnerability to cyberattacks.** The growth in online banking and remote work since the onset of the pandemic has increased banks' dependence on digital technology to serve customers. It has also expanded their use of virtual private networks (VPNs) and similar applications and services to support their remote work forces. Banks have quickly responded to these challenges, but in pursuing an accelerated technology development cycle have also increased their potential vulnerabilities to cyberattack.

» **External actors seeking financial gain are the mostly likely cyber actors to target banks.** External actors have been the largest perpetrators of cyberattacks on the financial sector, causing 64% of data breaches compared with 35% by internal actors. Cyber actors most often are trying to get easily monetized data (77% of data breaches),[2] as illustrated by the fact that wire fraud transfer remains the most common cyberattack vector.[3]

» **Banks have developed good cyber risk awareness and mitigation measures.** Banks mitigate cyber risk through three primary mechanisms. The first is strong corporate governance, including enterprise-wide cybersecurity frameworks, strategy and policy enforcement and improved reporting. The second is risk prevention and response and recovery readiness. And the third is information-sharing with other banks, adoption of international standards and regulatory oversight. These measures in combination have improved banks' cyber-readiness to a level above that of most other sectors.

Large-scale shift to digital banking and remote work increases banks' vulnerability to cyberattacks

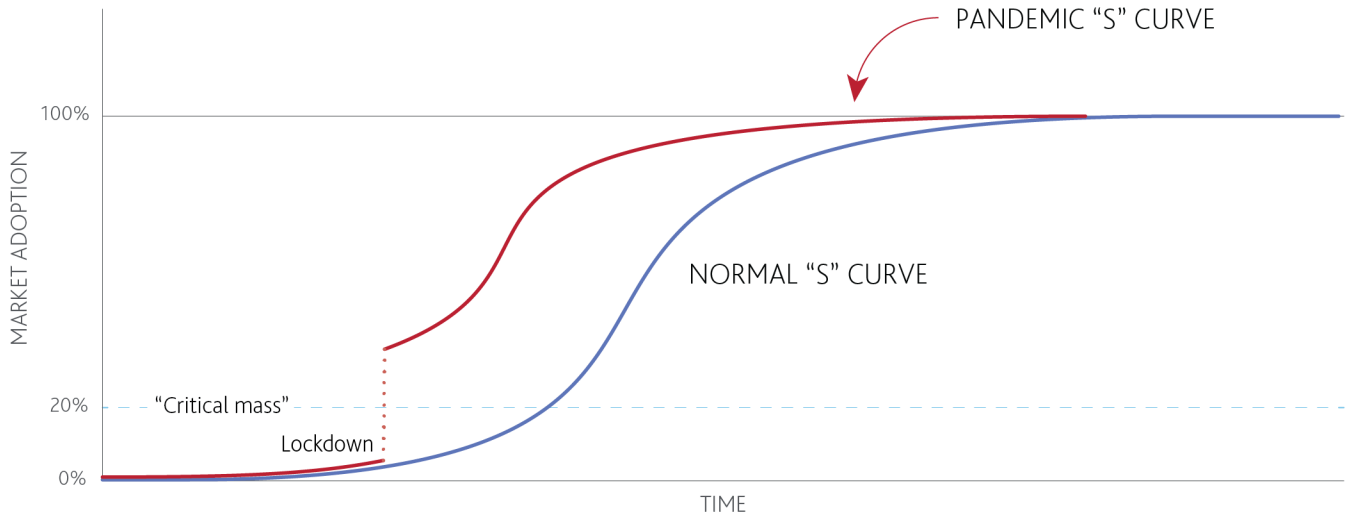
Social restrictions to help contain the public health threat from the coronavirus outbreak have been a powerful catalyst of accelerated migration to digital online banking, both by businesses and consumers. Additionally, the widespread implementation of remote work during the pandemic will likely lead to more bank employees working from home on a regular and long-term basis. Both developments will help increase banks' productivity but will also increase vulnerability to cyberattack.

Social distancing has created a surge in demand for contactless payments, digital cash transfers and online banking. Corporate and retail banking customers that have newly or more fully converted to digital banking will come to appreciate and expect better user experiences and will not likely fully return to brick-and-mortar banking once restrictions on in-person transactions are fully lifted. Corporate customers will want to retain new efficiencies and cost savings, and retail customers will be more attached to the enhanced functionality and usability of online banking apps. These structural changes will have an immediate and long-lasting impact on banks' businesses, establishing a new "S" curve for digital adoption and accelerating the typical technology adoption cycle in the coming years (see Exhibit 1).

Exhibit 1

Social distancing has caused a surge of new users for some technologies

Effect of social distancing and lockdowns on idealized digital technology adoption curves



Source: Moody's Investors Service

Beyond the coronavirus-led surge in digitalization, the underlying adoption of technology continues apace: business decisions are increasingly data-driven across all banks' business lines. In retail banking, the proliferation of mobile banking, new "open banking" regulation and data-sharing with third-party providers (such as consumer credit firms and retailers) will greatly increase the quantity and exposure of client data. In the capital markets business, banks' IT architecture is expanding into a "technology hub" model, leading to greater interconnectedness with technology firms.

Meanwhile, the proven efficacy of remote-work technologies for teleconferencing and digital collaboration will make it possible for banks to use remote work arrangements as a lever to reduce costs in expense-heavy, data-based businesses in which most work can be done outside the office.

However, the increased productivity that digital banking and remote work bring also comes with increased cyber risk exposure:

Greater demand for and dependence on digital banking technology has increased the risk of successful cyberattacks by increasing the strains on banks' critical IT infrastructure through the rapid rollout of new digital solutions for customers. Banks' new digital customers are a natural target for fraudsters through 'phishing' emails (for example, emails that look like they are from the bank and that may be about financial support available for coronavirus, but which lure customers to provide their account information) or social engineering (for example, social-media games luring customers to provide information that hackers then use to impersonate the customer with their bank). Banks can reduce these risks by introducing additional layers of authentication or authorization.

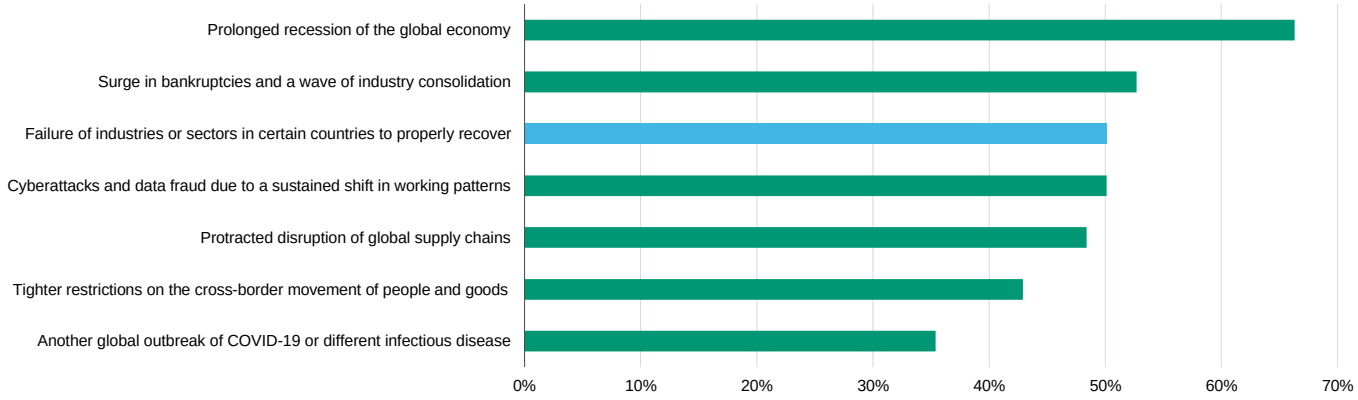
The increase in remote work has also increased the risks of successful cyberattacks: home devices used to access office networks are more likely to be or become infected with malware or spyware; unsecure home Wi-Fi networks may use routers with weaker security. There is also a higher risk of "spoofing" email scams: for example, a hacker impersonates a company manager to trick the employee into making payments, usually by wire transfer: if employees are not in the office, they are usually less suspicious of such requests. VPN software products also have a host of security issues: some cybercriminals target organizations specifically through vulnerabilities in their VPN products, which sometimes are not configured with multifactor authentication or have a password that can be guessed or phished.

The increased vulnerability of financial institutions is evident from a 238% increase in cyberattacks between February and April 2020, as coronavirus spread across the globe, and a ninefold increase in ransomware attacks on the sector over the same period, both according to a report from VMware Carbon Black[4]. The cybersecurity company also reported an 80% increase in cyberattacks over the past 12 months among surveyed financial institutions. In addition, 82% of surveyed financial institutions said cybercriminals are more sophisticated, leveraging advanced tactics, techniques and procedures, and social engineering attacks such as phishing credentials, distributed denial of service (DDoS) and pretexting to hide malicious activity.

Corporate managers are well aware of the cyber threat. According to a recent report from the World Economic Forum[5], the fourth most worrisome fallout for companies from the spread of coronavirus is an increase in cyberattacks and data fraud (see Exhibit 2).

Exhibit 2

Most worrisome fallout for companies resulting from spread of coronavirus



Source: World Economic Forum: "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications", May 2020

External actors seeking financial gain are the most likely cyber actors to target banks

Cyberattacks in the financial sector are mostly perpetrated by external actors (64% of data breaches), mostly through web applications and errors made by company employees, according to a recent report by Verizon[6]. The major motivation is to get easily monetized data (77% of data breaches) (see Exhibit 3).

Exhibit 3

Summary of cyber breach findings for financial institutions

Top Patterns	Web Applications (c.30%), Errors (c.30%), Others (c.20%)
Threat	Actors External (64% of breaches), Internal (35%) Partner (2%), Multiple (1%)
Actor Motives	Financial (91% of breaches), Espionage (3%), Grudge (3%)
Data Compromised	Personal (77% of breaches), Other (35%), Credentials (35%), Bank (32%)

Source: "Verizon, Data breach report 2020", May 2020

Top patterns

Cyber incidents and data breaches follow a number of different patterns (see Exhibit 4). Web application attacks and employee errors are the major causes of breaches, each accounting for around 30% of breaches. Employee errors take various forms. The most common error is mis-delivery, in which information such as electronic data is sent to the wrong recipient. The second most common error is misconfiguration, in which a system administrator misconfigures firewall settings or does not secure cloud storage. Other errors include email compromises and phishing attacks (or a combination of both) and social engineering techniques; that is, situations manufactured to convince the target to transfer money to the attacker's bank account.

Exhibit 4

Classifications of incidents / data breaches

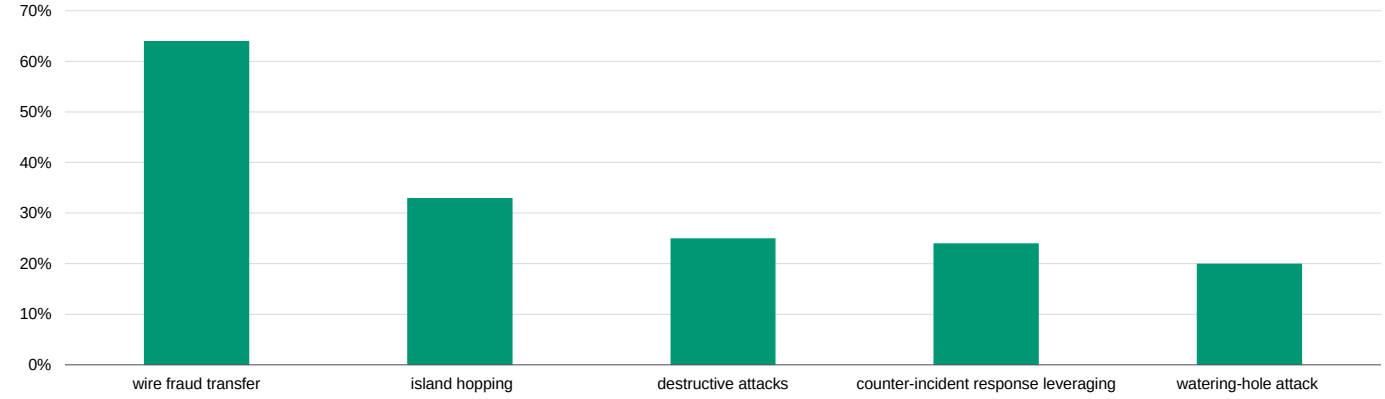
Hacking	Social	Error	Malware	Physical
•Use of stolen credentials •Exploit vulnerability •Use of backdoor •Abuse of functionality •SQLi	•Phishing (credential, personal, internal, medical, bank) •Pretexting	•Misconfiguration •Mis-delivery •Publishing Error	•Password dumper •Capture app data •Ransomware •Downloader •Trojan •Capture stored data •Export data •Exploit vulnerabilities •Scan network •RAM scraper	•Server (through web apps, mail, database) •User device (desktop/ laptop) •Person (end-user)

Source: Moody's and "Verizon, Data breach report 2020"

According to VMware Carbon Black, the most common cyberattack vector is **wire fraud transfer** (see Exhibit 5), which targets employees and clients directly through social engineering or exploits gaps in the wire transfer verification process. For example, cyberthefts can take advantage of banks' poor controls and security practices for connecting to payment systems. These systems include the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, the mainstream messaging system used by more than 11,000 member financial institutions in more than 200 banking systems for financial transactions[7]. Other cyberattack vectors include **island hopping** (partners and supply chains are hijacked to target the primary firm), **destructive attacks** (aiming to destroy data), attacks leveraging **counter-incident response** and **watering-hole** attacks, in which the web site of a financial institution or regulator is hijacked to infect visitors' browsers.

Exhibit 5

Cyberattack vectors during the last year for surveyed financial institutions



Source: VMware Carbon Black "Modern Bank Heists 3.0", May 2020

Threat

The majority of attacks in this sector are perpetrated by external actors (64%), followed by internal financially-motivated actors (18%) or facilitated by internal actors committing errors (9%). Most attacks on financial institutions are perpetrated by cybercriminals, although there is a small amount of cyberespionage by state actors or nations.

Motives

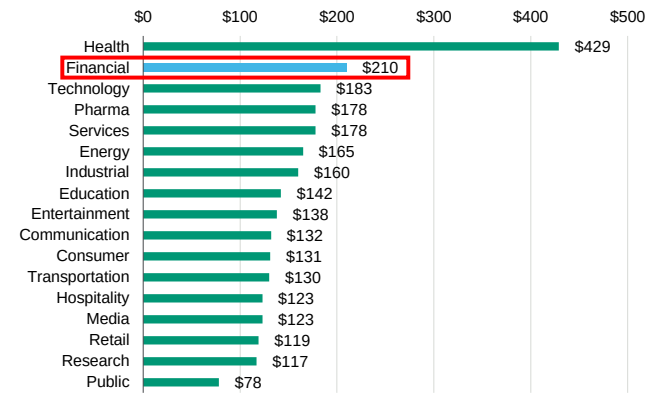
Cyber actors are mostly financially motivated (91% of total) to access easily monetized data stored by the victim organizations.

Data Compromised

Cyberattacks have various, and sometimes multiple, goals but the vast majority target personal data (77%), with a minority focused on credentials (35%) and bank data (32%). Because personal customer data is involved, the average cost of a breach per record in the financial sector is $210,000, the second highest amount after the health sector[8] (see Exhibit 6). The average overall cost of a data breach for the financial sector is $5.9 million, second only to that in the health sector (see Exhibit 7).

Exhibit 6

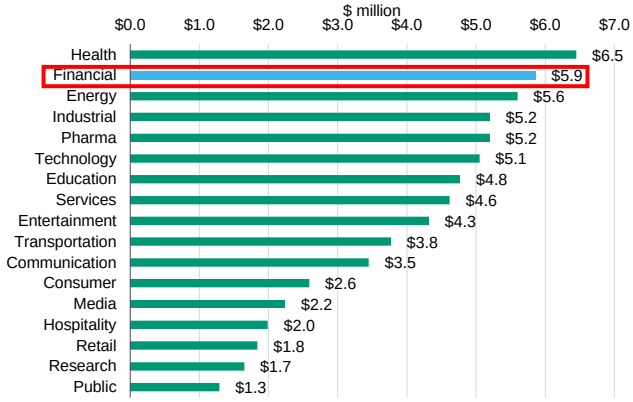
Average cost per file record by industry sector



Source: IBM Security: Cost of a Data Breach Report 2019

Exhibit 7

Average total cost of a data breach by industry



Source: IBM Security: Cost of a Data Breach Report 2019

Banks have developed good cyber risk awareness and mitigation measures

Banks' have built strong cyber risk mitigants, including strong corporate governance; risk prevention and response and recovery readiness; and information-sharing and third-party oversight.

Corporate governance

Banks have significantly improved governance around cyber risk in recent years.

» **Cyber function structure and reporting lines.** Cybersecurity has become a a critical role in the organization, with visibility within the C-suite and, in turn, within the board of directors for many banks. This is important to ensure organizations allocate sufficient budget to information security and to make certain that management will be appropriately engaged during a crisis.

» **Enterprisewide cybersecurity framework.** The cybersecurity function has a prominent platform to manage and escalate issues, including discussing the implications of new business initiatives and ensuring that key leaders in the organization understand what cyber deficiencies exist and how they are being addressed.

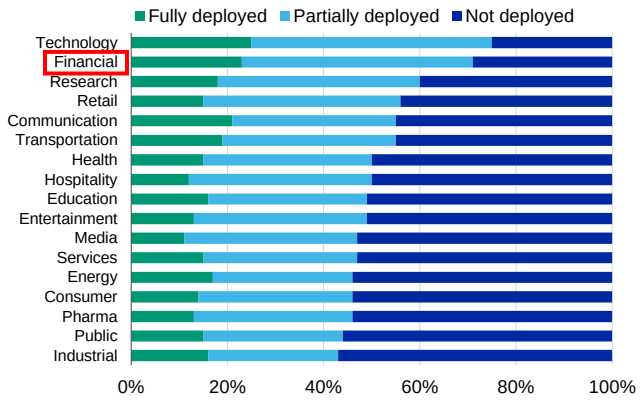
» **Board oversight of cyber risk.** The information security role typically provides regular reporting to the board. Often, cyber reporting includes some time for education sessions, which could be a deep dive on a particular cyber risk area, a review of a recent industry or global incident, or a cyber incident tabletop exercise.

» **Improved reporting:** according to our report on cyber risk disclosure[9], banks (together with telecommunications & media companies) provide the most detailed disclosures among the sectors analyzed. They go beyond citing cyber risk and their board oversight practices, and discuss in fairly specific terms their cybersecurity risk management strategies.

Risk prevention, response and recovery readiness

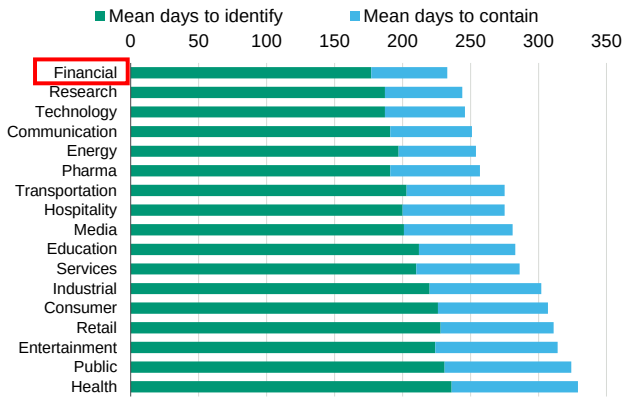
Banks have developed increasingly sophisticated tools to prevent cyber risk, raising cybersecurity automation in the financial sector above that in other sectors (see Exhibits 8 and 9):

Exhibit 8
State of security automation



Source: IBM Security: Cost of a Data Breach Report 2019

Exhibit 9
State of security automation



Source: IBM Security: Cost of a Data Breach Report 2019

Examples of banks' increasingly robust cyber risk prevention tools include:

» **Infrastructure security management** covers a wide range of measures, including end-point protection, prevention of unauthorized installations, system and data backups, physical security, contingency planning for cybersecurity scenarios and third-party service providers.

» **Network segmentation** is an effective way to limit exposure from phishing attacks and compromised networks. The bank's computer network is segmented into different zones so as to limit a hacker's ability to move laterally across the network.

- **Strong user access management** helps lower the risk of cyberattacks that infiltrate bank networks by stealing access privileges via privilege escalation, remote access, social engineering and data exfiltration. This involves segregation of access privileges, the provisioning and de-provisioning of identities, securing and authentication of identities, and the authorization to access resources so as to prevent malicious use of stolen credentials.
- **Cloud-based cybersecurity** can enable quicker, more effective adaptation to the changing nature of cyberattacks. Cloud computing also offers flexibility because major cloud security providers have large resources and heightened resilience to cyberattacks. Banks have also invested in cloud cyber defenses; for example, encrypting and tokenizing customer data, among other strategies.
- **Use of artificial intelligence and penetration tests.** More banks use data mining tools and artificial intelligence to detect fraud and other anomalies in security breaches. Other widely adopted prevention tools include regular penetration testing on banking networks to find security vulnerabilities that cyberattackers could exploit.

Information sharing, adoption of international standards and regulatory oversight

- **Information-sharing on attacks has increased between large financial institutions.** Many large banks benchmark against each other, mostly through the use of external parties, such as firms specialized in cyber analysis and deterrence, as well as consultancy firms. In addition, the industry increasingly conducts exercises in which in-house and external experts attempt to hack systems to identify potential vulnerabilities.
- **Adoption of international standards.** The two particular standards banks reference as preferred are the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and the Committee on Payments and Market Infrastructures — Board of the International Organization of Securities Commissions (CPMI-IOSCO) Guidance on Cyber Resilience for Financial Market Infrastructures.
- **Cyber regulation has increased for banks.** Regulators have comprehensive frameworks to promote banks' cyber-resilience, including supervisory assessments as part of their risk-based supervisory activities. Compliance with the European Union (EU) General Data Protection Regulation (GDPR)[10] has also increased standards for customer data protection.

Moody's related publications

Cyber risk

Banking sector:

» Cyber Risk – Global Investment Banks: GIBs heighten readiness against constant cyber threat, 7 October 2019

» Retail and Commercial Banks – Global Growing digitalization increases banks' cyber risk exposure, 21 October 2019

» Market Infrastructure Providers and Securities Cos – Global: Rising cyber risk of highly interconnected firms has systemic implications, 17 October 2019

Cross sector:

» Cross-Sector – Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects, 28 February 2019

» Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, 2 October 2019

Corporate sector:

» Corporates – Global Suppliers and vendors are becoming the weakest link in corporate cybersecurity, 8 June 2020

Digitalization

Sector Comment:

» Financial Institutions – Global: The coronavirus experience will likely change habits and reshape business models, 19 May 2020

» Banking – Europe: Lockdowns drive surge in the use of digital banking channels and remote working, 17 June 2020

Sector In-Depth:

» Banks – Spain: Digitalisation brings competition, higher costs and eventually, efficiency, 11 March 2020

» Fintech - Global Investment Banks: GIBs can keep pace with fintechs, but retail banking is most at risk of a digital divide, 19 February 2020

» Banks – US: Large banks benefit from rapid digitization and the diminishing need for branch density, 13 January 2020

» Fintech – France: French banks invest heavily to maintain dominance in the new digital world, 19 November 2019

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 See Moody's report: **The coronavirus experience will likely change habits and reshape business models**, 19 May 2020

2 "Verizon, Data breach report 2020", May 2020

3 VMware Carbon Black "**Modern Bank Heists 3.0**", May 2020

4 VMware Carbon Black **"Modern Bank Heists 3.0"**, May 2020

5 World Economic Forum: "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications", May 2020

6 "Verizon, Data breach report 2020", May 2020

7 See Moody's report: "Retail and Commercial Banks – Global: Growing digitalization increases banks' cyber risk exposure", October 2019

8 Source: IBM Security: Cost of a Data Breach Report 2019, 2019

9 Cyber Risk – Global: Cyber disclosures reveal varying levels of transparency across high-risk sectors, 2 October 2019

10 GDPR is designed to harmonize data privacy laws across Europe. The regulation applies to any organization that holds data on EU citizens, regardless of where the data is stored or domiciled and requires these organizations to make it clear in what ways they use customers' data, with whom the data is shared, and that data passed on to third parties is handled according to GDPR requirements. Companies that fail to comply with GDPR could face fines up to 4% of global revenue

REPORT NUMBER 1235294

Contacts

Alessandro Roccati +44.20.7772.1603
Senior Vice President
alessandro.roccati@moodys.com

Lesley Ritter +1.212.553.1607
VP-Senior Analyst
lesley.ritter@moodys.com

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

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