# Cyber Risk Insights: New Regulations Will Increase Resilience, At A Cost

**August 3, 2023**

## Key Takeaways

- New and emerging legislation dictating cyber-related disclosure and governance standards could weigh on issuers' financial risk profiles by increasing the likelihood of penalties and by necessitating investment to meet minimum standards.
- Stricter disclosure requirements will also reveal differences in cyber preparedness and could be a differentiating factor in S&P Global Ratings' risk and governance assessments, which contribute to our view on issuer credit worthiness.
- The EU and U.S. have taken a lead in introducing and enforcing cyber regulations. Their practices are influencing the formulation of laws in other regions.

Regulators are shining a spotlight on organizations' cyber exposure by demanding greater disclosure of cyber-related events, their impact, and information on organizations' cyber preparedness and resilience. The main aim is to enforce minimum standards and ensure company's assume responsibility for their own cyber security. Yet greater insight is also opening the door to differentiation based on cyber risks, which could have implications for company credit worthiness.

The reason for this growing demand for transparency is no mystery. Cyber criminality, which accounts for most cyber attacks, is growing and is increasingly sophisticated both in terms of tactics and technology. That is enabling criminals to increase both the cadence of their activity and to monetize their activities more aggressively. The number of cyber breaches, defined as an incident that results in confirmed disclosure of data to an unauthorized party, has more than doubled in the past five years (see chart 1), and become increasingly costly (see chart 2).

PRIMARY CREDIT ANALYST

**Vishal H Merani, CFA**
New York
+ 1 (212) 438 2679
vishal.merani
@spglobal.com

SECONDARY CONTACTS

**Martin J Whitworth**
London
+44 2071766745
martin.whitworth
@spglobal.com

**Paul Alvarez**
Washington D.C.
+1 2023832104
paul.alvarez
@spglobal.com

**Michael V Grande**
New York
+ 1 (212) 438 2242
michael.grande
@spglobal.com

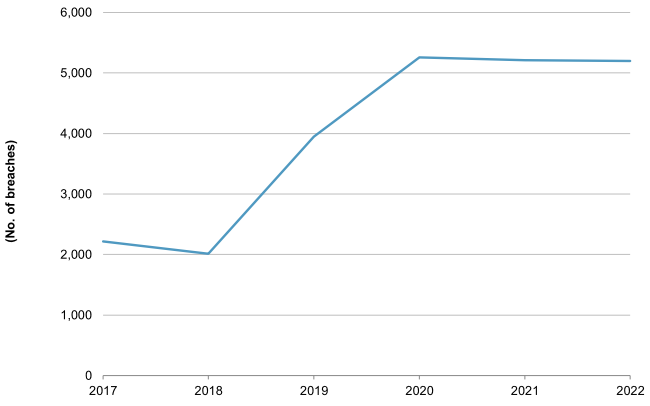
**Patrick Bell**
New York
(1) 212-438-2082
patrick.bell
@spglobal.com

**Minesh Shilotri**
San Francisco
+ 1 (415) 371 5064
minesh.shilotri
@spglobal.com

**See complete contact list at end of article.**

Chart 1

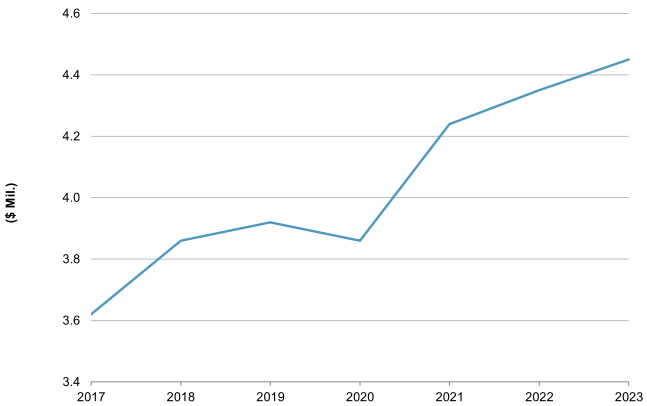
**Data breaches have more than doubled in the past five years**
Global data breaches (including the public sector)*




*All figures are for the 12-months to the end of October in the cited year. Totals are for all sectors, including public sectors. Source: Verizon DBIR reports 2018-2023.


Chart 2

**The average cost of a data breach is increasing**
Global average data breach cost*




*All figures are for the 12-months to the end of March in the cited year. Source: IBM Cost of Breach report 2023.


## The Legislative Response

Organizations have been forced to respond to the growing threat. Spending on global information security and risk management was estimated at about $169 billion in 2022, up from $158 billion a year earlier, according to an October 2022 report by Gartner, a technology consulting company. That figure could grow to about $188.3 billion over 2023, according to Gartner. Companies are also increasingly purchasing cyber insurance to offset costs from cyber incidents. Premiums for cyber insurance reached about $11.9 billion in 2022, up from $5.8 billion in 2019, according to Munich RE, an insurer, which projected a total $33.3 billion in annual spending on cyber insurance by 2027.

It isn't only the targets of cyber crime that are reacting. Governments have met the increasing cyber threat with a growing raft of legislation that seeks to protect critical infrastructure and consumer data, force organizations to bolster cyber defenses, and ensure greater disclosure of cyber events and cyber-risk factors.

This drive to legislate cyber-risk management has been led by larger developed countries, most of which have enacted regulation covering data privacy and critical infrastructure. At the forefront are the U.S. and Europe (see chart 3), which have proven willing to both impose regulations and levy fines against transgressors. Their lead is likely to influence the formulation and enforcement of regulation in other regions over the coming years, when we expect countries will tighten regulations and implement new rules. A summary of significant global cyber regulations is included as an appendix.

Chart 3

### Cyber regulations across the world

| | Data privacy | Critical infrastructure | Other |
|---|---|---|---|
| **North America** | | | |
| U.S. | • Health Insurance Portability And Accountability Act (HIPAA)<br>California Consumer Privacy Act (CCPA) | • Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) | • Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure<br>Quality System Regulation (QSR) For<br>• Medical Devices and Section 3305 of Medical Services |
| Canada | • Personal Information Protection and Electronic Documents Act (PIPEDA) | | |
| **EMEA** | | | |
| Europe | • EU General Data Protection Regulation (GDPR) | • Network and Information Security Directive (NIS2)<br>• Digital Operational Resilience Act (DORA) | |
| U.K. | • Data Protection Act | | |
| **Latin America** | | | |
| Brazil | • Brazilian General Data Protection Law (LGPD) | • Resolution N 740, 2020 (R-Ciber) | |
| **Asia-Pacific** | | | |
| Australia | • Australia Privacy Act | • Telecommunications Sector Security Reforms (TSSR) Security of Critical<br>• Infrastructure Act (SOCI) | • Criminal Code Act |
| Japan | • Basic Act of Cybersecurity (BAC)<br>• Act on the Protection of Personal Information (APPI) | • Act on the Promotion of National Security through Integrated Economic Measures (ESPA) | |

Source: S&P Global Ratings.


## Cyber Regulation And Credit Risk: The Downside

Cyber risk is inherently credit negative. Issuers are exposed to significant loss and business disruption in the event of a major incident, as well as fines and other penalties due to insufficient cyber preparedness. Yet even excellent cyber-risk management will, at-best, enable an organization to continue its usual course of operations.

That inherent negativity reflects the fact that cyber preparedness doesn't typically create value and can be costly. Furthermore, cyber-related expenses are likely to increase as threats evolve and proliferate, and thus demand increased investment in external resources, new technologies, new systems, and personnel.

Increased cyber regulation, coupled with more vigorous enforcement, could exacerbate cyber risks' negative bias by adding new fines and other sanctions to the potential damage resulting from cyber issues. New rules could also necessitate further investment in systems and technology. For example, regulations already in place (including GDPR in Europe and CCPA and HIPAA in the U.S.) require timely disclosure of a cyber attack to regulators and affected individuals. That makes investment in effective detection systems crucial to avoiding penalties--though the same systems can also deliver benefits in terms of avoiding excessive damage following a breach (see "Cyber Risk Insights: Detection Is Key To Defense," May 10, 2023).

Investment in new systems may also be required to satisfy regulations designed to protect critical infrastructure, improve national security coordination, and inform financial markets. Critical infrastructure and security rules, such as CIRCIA in the U.S. and NIS2 in Europe, typically require disclosure to central agencies within a defined time-period and include penalties for entities that fail to meet the minimum standards. The SEC, meanwhile, recently finalized new "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" rules for public companies. The rules will impose one-time and ongoing compliance costs and will likely accelerate investment in cyber risk governance and preparedness for companies that have not already sufficiently invested in these areas.

Cyber regulation could also indirectly weigh on organizations' operations, liquidity, and profitability. For example:

- New cyber security standards could lengthen and complicate product approval for developers and manufacturers, as has been the case in the U.S. where section 3305 of the regulation for medical devices has put the onus on device makers to patch and update products.
- Increased regulatory emphasis on security by design could expose organizations to responsibility for damage incurred due to exploitation of security flaws in their products or services.
- An increasing burden of care with regards to data protection could weigh on sectors that regularly collect and use personal data, such as e-commerce, retail, telecommunications, healthcare, and financial services.
- Greater restrictions on access to some consumer data could adversely impacts business models or service/product functionality.
- Due to an increase in the cost of cyber insurance in response to wider and more complex regulations and a greater threat of penalties and litigation. Insurers are also likely to respond by raising their minimum cyber hygiene standards for policy holders, further increasing cyber-related costs for issuers.

## Cyber Regulations And Credit Risk: The Upside

Increased cyber-related regulation should also have some positive impacts on credit risk. Most evidently, organizations' response to a stronger regulatory stance is likely to increase their investment in and ability to identify and respond to issues that emerge. This should reduce the potential for cyber-incident losses that are sufficient in magnitude to negatively affect credit quality.

Issuers also stand to benefit from additional government agency support, such as that offered by the U.S.'s Cybersecurity and Infrastructure Security Agency (CISA). That support should contribute to better identification (and thus avoidance) of threats, while also improving strategies to resolve issues. Also, regulators' facilitation of knowledge sharing among organizations should serve to improve best practices relating to cyber risk management and governance.

And organizations stand to benefit from the growth of cyber security services, the provision of which should expand due to increased demand (though there may also be near-term expertise shortages). As new investment flows into the cyber security sector services should improve and technology should become more effective, with benefits for both clients and wider business sectors.

## A Differentiating Factor

It is inevitable that greater regulatory scrutiny of cyber risk factors will bolster disclosure of both cyber incidents and the extent to which organizations adopt good cyber hygiene. Greater visibility into cyber incidents will provide new insights into corporate governance and risk management, and improve the comparability of how cyber risk affects organizational risk and is dealt with in terms of management and governance.

This will continue to augment our ability to differentiate issuers based on cyber risk preparedness as a part of their overall risk management framework and, ultimately, be reflected in our ratings. Meanwhile, enforcement actions, such as fines for substandard cyber hygiene resulting in cyber breaches, could also impact our view of issuers' credit worthiness.

Because much cyber regulation is relatively new, it remains to be seen to what extent the information produced will prove valuable to credit-quality assessment. It is also unclear to what extent fines, and the imposition of other costs due to regulatory demands, might weigh on credit worthiness--not least because that will be contingent on how aggressively regulators enforce rules.

## Cyber Preparedness and Regulatory Compliance Influence Credit Risk

Analysis of cyber risk management is embedded within our assessment of entities' management and governance, which is itself a key factor in our consideration of credit quality (see "Cyber Risk Insights: Navigating Digital Disruption," Feb. 22, 2023).

New cyber regulations, and the evolution of existing rules, means regulators will inevitably drive changes in the way that organizations' manage cyber risk, including by dictating norms of preparedness, reporting, and the manner in which cyber incidents are addressed. That will prove burdensome. Cyber preparedness budgets are likely to grow due to increased complexity and new investment needed to comply with regulations and to mitigate the risk of regulatory censure. We expect cyber risk managements average share of companies' I.T. budgets to grow from current levels of about 10%.

Yet new regulation and enforcement could prove beneficial in addressing risks to credit worthiness. Rules that improve cyber hygiene and reduce the potential for significant losses should strengthen companies, both at an individual level and by raising the standards of the ecosystems in which they operate. New penalties coupled with increased governance and disclosure requirements could incentivize companies to accelerate cyber investments and reduce the risk associated with cyber events.

Meanwhile, a backdrop of more frequent and costly cyber-incidents, and regulations requiring companies to bolster prevention, disclosure, and responsiveness, supports the case for cyber risk preparedness to increasingly become a differentiating factor in credit quality assessment.

## Appendix: Significant Global Cyber Regulations

### North America

## U.S.

### Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

**Timing:** Enacted in March 2022. Final regulatory requirements expected September 2025.

**Regulatory Body:** Cyber security and Infrastructure Security Agency (CISA)

**Scope of the regulation:** CIRCIA requires critical infrastructure companies to report cyber security incidents to CISA within 24 or 72 hours, depending on the event. Critical Infrastructure sectors include chemicals, commercial facilities, communications, certain manufacturing industries with national significance, dams, defense, emergency services, energy, financial services, food and agriculture, government facilities, healthcare, information technology, and waste. Proposed rules don't currently define a materiality threshold for cyber security incidents and, while the regulations are being finalized, companies are encouraged to voluntarily report incidents with CISA.

### Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

**Timing:** The SEC adopted the rule on July 26, 2023. Final rules will become effective 30 days after publication of the adopting release in the Federal Register. 8-K disclosure of cyber incidents becomes applicable on the later of Dec. 18, 2023, or 90 days after publication in the federal register. 10-K disclosure of cyber-risk management process and updates on previously disclosed incidents becomes applicable for annual reports with fiscal years due Dec. 15, 2023, or later.

**Regulatory Body:** Securities Exchange Commission (SEC)

**Scope of the regulation:** The rules aim to inform investors about a company's risk management, strategy, and governance, and to provide timely notification of material cyber-security incidents.

Specific requirements include the reporting of a material cyber-security incident (Form 8-K) within four business days after the company determines that it has experienced a material incident. Companies will also be required to disclose when previously undisclosed immaterial cyber-security incidents become material in the aggregate. Disclosures include the nature, scope, and timing as well as the impact from the incident.

Standardized disclosures in annual filings (10-K and 20-F) include processes used by companies in assessing, identifying, and managing material risks from cybersecurity threats, material effects or risks from cybersecurity threats, and updates from previous cyber-security incidents. Disclosure requirements also include board oversight of, and managements role and expertise in assessing and managing cyber-security threats.

### The Health Insurance Portability and Accountability Act (HIPAA)

**Timing:** Enacted in 1996.

**Regulatory body:** Department of Health and Human Services Office for Civil Rights (HHS)

**Scope of the regulation:** HIPAA applies to health care providers, health plans, and health care clearinghouses (the covered entities). It consists of three main sections. The "Privacy Rule" establishes national standards to protect individuals' medical records and other individually identifiable health information. The "Security Rule" sets security standards to protect personal health information held or transferred in electronic form, and addresses technical and non-technical safeguards that must be put in place. The "Breach Notification Rule" requires a covered entity notify the HHS Secretary if a breach of unsecured protected health information is discovered.

**Penalties:** 875 breaches affecting about 75 million individuals were reported in the two years to July 3, 2023. Maximum civil penalties are $50,000 ( up to an annual maximum of $1 million) for HIPAA violations due to willful neglect and which are not corrected.

## Quality System Regulation (QSR) For Medical Devices And Section 3305 of Consolidated Appropriations Act

**Timing:** QSR has applied to medical device software since the late 1970s and incorporated cyber security since 2005. Section 3305 was enacted in December 2022.

**Regulatory body:** The Food and Drug Administration (FDA).

**Scope:** QSR applies primarily to medical device original equipment manufacturers (OEMs) attempting to sell products in the U.S. It defines the requirements device manufacturers must follow to protect connected medical devices from cyber criminals, including software patching in response to identified vulnerabilities. Section 3305 authorizes the FDA to implement and enforce new cyber-security standards for premarket submissions of medical devices to ensure they are secure when they are introduced to the market. Premarket applications must include a plan to monitor, identify, and address post-market cyber-security vulnerabilities and exploits and include coordinated vulnerability disclosures and related procedures.

**Penalties:** QSR violations can incur fines of up to $500,000. Section 3305 fines can be up to $15,000 per incident (capped at $1 million). Non-compliant manufacturers may be considered in violation of medical device application regulations.

## California Consumer Privacy Act (CCPA)

**Timing:** Enacted Jan 2020.

**Regulatory body:** Attorney General for the State of California and private litigants.

**Scope:** The CCPA provides Californian consumers statutory rights to learn what personal information businesses have collected, sold, and disclosed, as well as the right to request deletion of their information, opportunities to opt-out of the sale of their personal information, and protection from discrimination in the form of reduced service or functionality for exercising those rights. The law applies to any companies that does business in California and has more than $25 million in revenue, buys or sells the personal information of 50,000 or more consumers, or derives half or more of its annual revenue from selling consumers' personal information.

**Penalties:** Civil penalties of as much as $2,500 for each violation, or $7,500 for each intentional violation after notice and a 30-day opportunity to cure have been provided. The statute also allows for civil damages of $750 per affected user.

## Canada

### Personal Information Protection and Electronic Documents Act (PIPEDA)

**Timing:** Enacted April 13, 2000 and implemented in three stages from 2001 through 2004.

**Regulatory body:** The Office of the Privacy Commissioner of Canada.

**Scope of the regulation:** Any private organizations in Canada that collects personal information (including employee information) during commercial activity is subject to PIPEDA. The act requires businesses to follow 10 fair information principles to protect personal information, including identifying someone responsible for compliance, identifying and documenting the purpose of collecting information, and obtaining consent for collection and storage of data. The Federal Court of Canada has also ruled that PIPEDA should apply to businesses operating outside of Canada if there is "a real and substantial connection between the foreign organization and Canada and a physical presence is not required."

**Penalties:** Currently none. Canada is developing a new Consumer Privacy Protection Act (CPPA) which includes administrative penalties of the higher of three percent of gross global revenue or $7.6 million (CAD 10 million), and the higher of five percent of gross global revenue or $19 million for serious contraventions of the law.

# EMEA

## Europe

### EU General Data Protection Regulation (GDPR)

**Timing:** Entered into force in May 2016 and applied since May 2018.

**Regulatory body:** Each EU member state has a Supervisory Authority (or Data Protection Authority) tasked with supervising and enforcing GDPR compliance. A representative from each national Supervisory Authority sits on the European Data Protection Board (EDPB), which oversees the consistent and effective application of the GDPR across the EU.

**Scope:** The purpose of the GDPR is to create a uniform and harmonized level of protection for personal data within the European Union. It sets out rules for data protection and privacy for all individuals (data subjects) within the EU and regulates how physical or legal persons, wherever they are located, may process the personal data of data subjects in the EU. GDPR requires companies to report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach.

**Penalties:** National authorities assess penalties for specific data protection violations in accordance with the GDPR, which sets a maximum fine of the greater of €20 million or 4% of annual global turnover. Supervisory authorities can also take other actions including issuing warnings and reprimands; temporary or permanent bans on data processing; ordering the rectification, restriction, or erasure of data; and suspending data transfers to third countries.

## Network and Information Security Directive (NIS2)

**Timing:** Entered into force in January 2023, while EU member nations have until October 2024 to transpose its measures into national law.

**Regulatory body:** Each member nation has one or more competent authorities (and one nominated point of contact) responsible for supervising, and enforcing NIS2 compliance.

**Scope:** The EU-wide legislation on cyber security updates previous EU cyber security rules and provides legal measures to boost the overall level of cyber security in the EU. NIS2 includes rules requiring member nations to be appropriately equipped, for example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority. It also established a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among member nations. And seeks to foster a culture of security across vital sectors that rely heavily on information and communications technology, such as energy, transport, water, banking, financial markets, healthcare, and digital infrastructure.

Under NIS2, affected companies have 24 hours from the time they become aware of an incident to submit an early warning to the competent national authority and request assistance if required. The early warning should be followed by an incident notification within 72 hours of becoming aware of the incident, and a final report no more than one month later.

**Penalties:** NIS2 requires member states to impose administrative fines that amount to the higher of €10 million ($11 million) or 2% of the total worldwide annual turnover of the preceding financial year for companies deemed essential, and €7 million or at least 1.4% of the total worldwide annual turnover of the preceding financial year for companies deemed important.

## Digital Operational Resilience Act (DORA)

**Timing:** DORA entered into force in January 2023 and will be effective from January 2025.

**Regulatory body:** Each EU member nation will have one or more competent authorities responsible for supervising and enforcing DORA compliance. Relevant European Supervisory Authorities (ESAs), such as the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA) will develop technical standards for financial services institutions (including banking, insurance, and asset management).

**Scope:** DORA is a key part of the European Commission's Digital Finance package and a significant regulatory initiative targeting operational resilience and cyber security at financial services entities and their technology providers. For financial entities, the regulation covers I.T. risk management, incident reporting, digital operational resilience testing, information and intelligence sharing, and management of third-party risk. Certain third-party technology providers

will be deemed critical service providers under DORA and will be subject to direct regulatory oversight.

**Penalties:** DORA imposes various penalties including administrative fines on financial institutions of up to the higher of €10 million or 5% of total annual turnover for serious infringements. Supervisory authorities may require financial institutions to take remedial measures to address any weaknesses or failures in their operational resilience. Penalties could also include withdrawal of authorization to perform business if the institution repeatedly fails to comply with the regulation, and it could require financial institutions to compensate customers or third parties for damages arising from non-compliance with the regulation.

## U.K.

### U.K. Data Protection Act 2018

**Timing:** Enacted in May 2018 and amended in January 2021.

**Regulatory body:** The Information Commissioner's Office (ICO).

**Scope:** The Data Protection Act is the U.K.'s implementation of the GDPR (see section on the EU General Data Protection Regulation). It sets out the key principles, rights, and obligations for most processing of personal data in the UK, excluding law enforcement and intelligence agencies. It is based on the GDPR and is, currently, practically identical.

**Penalties:** Similar to GDPR, maximum penalties are the higher of £17.5 million ($22.5 million) or 4% of the total annual worldwide turnover in the preceding financial year.

# Latin America

## BRAZIL

### Brazilian General Data Protection Law (LGPD) - Law No. 13,709

**Timing:** Enacted in 2018, in force since September 2020, and amended in August 2021 to add sanctions for non-compliance.

**Regulatory body:** The National Data Protection Authority (ANPD).

**Scope:** LGPD regulates Brazilian personal data processing, regardless of the means, the country of origin of the data, or the country where the processing takes place. The law applies to public and private companies' collection, transfer, storage, use, and deletion of personal data.

**Penalties:** Failure to comply with LGPD can result in a warning, fines up to the greater of 2% of a company's revenue or R$50 million (about $10 million), and suspension or prohibition of data processing.

### Resolution N 740, 2020 (R-Ciber)

**Timing:** July 2021

**Regulatory body:** National Agency of Telecommunications (ANATEL).

**Scope:** R-Ciber established guidelines for the implementation of cyber-security measures by telecommunication companies, with some exemptions for small providers. It includes guidance on risk management, incident response, and the protection of critical infrastructure, and requires companies to have a cyber-security policy, a cyber-security incident response plan, and to report any cyber-security incidents to ANATEL.

**Penalties:** Failure to comply with the R-Ciber regulation may result in fines and penalties, including suspension of operations, or revocation of the company's license to operate. R-Ciber applies to providers of telecommunications services with some exemptions for small-Size Providers.

## Asia-Pacific

## Australia

Australia Privacy Act 1988

**Timing:** The Privacy Act was introduced in 1988 and amended in 2014, 2017 and 2022.

**Regulatory body:** The Australian Cyber Security Centre (ACSC), which is part of the Australian Signals Directorate (ASD) and under the responsibility of the Minister for Cyber Security.

**Scope:** The Privacy Act is the principal piece of Australian legislation protecting the handling of personal information about individuals, including the collection, use, storage, and disclosure of personal information in the federal public sector and the private sector. Other state and federal laws that include cyber-security considerations, include the Criminal Code Act 1995, the Telecommunications Sector Security Reforms (TSSR), and the Security of Critical Infrastructure Act 2018.

**Penalties:** The maximum civil penalty is the greater of A$50 million ($33.5 million), three times the value of benefits obtained or attributable to the breach (if quantifiable), or 30% of the corporation's adjusted turnover during the "breach turnover period" (if quantifiable).

## Japan

### The Basic Act of Cybersecurity (BAC)

**Timing:** Enacted in 2014, in force since January 2015, with principal amendments in 2016 and 2018.

**Regulatory body:** The Cybersecurity Strategy Headquarters and the secretariat of the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC).

**Scope:** BAC defines cyber security as the measures necessary for the safe management of information. It includes the Cybersecurity Policy for Critical Infrastructure Protection's obligations for reporting and sharing of cyber security information in relation to critical infrastructure service providers. There are other laws that touch on cyber security and the protection of personal information. For example, the Act on the Protection of Personal Information (APPI), which was amended in 2022 to include mandatory reporting of personal data breaches (within 3-5 days for a preliminary report). The Act on the Promotion of National Security through Integrated Economic Measures (ESPA), which was approved by Diet (the national legislature of Japan) in August 2022 and will be gradually introduced by 2024. The Japanese government will require pre-screenings for infrastructure companies before new facilities are set up in well-defined core infrastructure sectors such as energy, water, communications, in order to protect critical infrastructure from cyberattacks and other threats.

**Penalties:** APPI includes scope for fines of up to 100 million yen ($700,000) for failure to comply with orders to rectify major data management system issues.

## Related Research

- Cyber Risk Insights: Detection Is Key To Defense, May 10, 2023
- Cyber Risk Insights: Navigating Digital Disruption, Feb. 22, 2023
- Cyber Risk In Health Care: High Stakes, Valuable Data, And Increasing Connectivity Attract Bad Actors, Dec. 6, 2022.
- Perspectives On Cyber Risk Across Corporates: The Potential Impact Of Cyber Threats Is Growing, Nov. 7, 2022.
- Cyber Risk Management Is Credit Risk Management, Says Seminar, Nov 01, 2022
- How Cyber Risk Affects Credit Analysis For Global Corporate Issuers, March 30, 2022.

Writer: Paul Whitfield

This report does not constitute a rating action.

## Contact List

PRIMARY CREDIT ANALYST

**Vishal H Merani, CFA**
New York
+ 1 (212) 438 2679
vishal.merani@spglobal.com

SECONDARY CONTACT

**Martin J Whitworth**
London
+44 2071766745
martin.whitworth@spglobal.com

SECONDARY CONTACT

**Paul Alvarez**
Washington D.C.
+1 2023832104
paul.alvarez@spglobal.com

SECONDARY CONTACT

**Michael V Grande**
New York
+ 1 (212) 438 2242
michael.grande@spglobal.com

SECONDARY CONTACT

**Patrick Bell**
New York
(1) 212-438-2082
patrick.bell@spglobal.com

SECONDARY CONTACT

**Minesh Shilotri**
San Francisco
+ 1 (415) 371 5064
minesh.shilotri@spglobal.com

SECONDARY CONTACT

**Diego H Ocampo**
Buenos Aires
+54 (11) 65736315
diego.ocampo@spglobal.com

SECONDARY CONTACT

**Richard Timbs**
Sydney
+ 61 2 9255 9824
richard.timbs@spglobal.com

SECONDARY CONTACT

**Makiko Yoshimura**
Tokyo
(81) 3-4550-8368
makiko.yoshimura@spglobal.com

SECONDARY CONTACT

**Maria Mercedes M Cangueiro**
Buenos Aires
+ 54 11 4891 2149
maria.cangueiro@spglobal.com