An Update on Cyber Legislation

Cyber risk continues to be a top concern for businesses, but new legislation designed to mitigate the risk is on the rise.

By Alex Wright

Regulators are taking a keen interest in cyber legislation as hackers continue to find crafty new ways into companies' systems.

As cyber risks increase in their frequency, severity and complexity, regulations governing how businesses and their risk managers deal with the problem are emerging in force.

Across the board, at global, federal and state levels, a host of new regulations — whether data breach notification or data privacy laws and statutes — have been brought forward in recent months, with more pending.

At the same time, regulators have been tightening up existing laws and clamping down more heavily on offenders when personal data is compromised, coming down squarely on the side of the consumer.

As a result, companies of all sizes are facing an unprecedented level of regulatory risk as they try to shore up their cybersecurity and protect their customers' data in the face of increasingly sustained and sophisticated cyberattacks by hackers.

This is a particular problem for firms that operate internationally and/or across multiple states, as well as smaller companies without the budget and resources needed to comply with these constantly evolving regulations.

"Every business will always have to face changing rules and regulations to security and privacy, whether specific industry trade sector bodies or countries they operate in, just as different cyber threat actors continuously seek to find new ways to impact an organization," said Scott Sayce, global head of cyber for Allianz Global Corporate and Specialty.

TIGHTER REGULATIONS

Among the most significant new pieces of legislation at the federal level is the Strengthening American Cybersecurity Act passed this year by the Senate and awaiting President Biden's sign-off.

The new law will require institutions deemed to be part of the U.S.'s critical infrastructure to report all data breaches and ransomware payments to the Department of Homeland Security within 72 hours of an incident's discovery and 24 hours of the payment, respectively.

"This is highly significant because it's the first time a single privacy statute has been brought in at the federal level seeking to encompass multiple different areas of industry," said Andrew Lipton, vice president and head of cyber claims at AmTrust Financial Services.

"This extends to financial services such as banks and insurance companies as well as key infrastructure players like utility companies and cloud service providers."

"Risk managers must stay informed on any changes in the collection, use, transfer and retention of personal information."

— Elizabeth Shirley, *co-chair, cybersecurity and data privacy team, Burr & Forman*

Then there are the proposed amendments to the Securities and Exchange Commission's rules on disclosures in terms of cybersecurity risk management, strategy, governance and incident reporting by public companies, also put forward this year.

This follows new data security rules introduced in October 2021 governing financial institutions regulated by the Federal Trade Commission (FTC), as well as a final rule issued by U.S. Banking Regulators in November 2021, requiring banks to report any material cybersecurity incident no later than 36 hours after determining it had occurred.

The FTC also issued guidance in January advising that any company failing to take into account a well-known vulnerability such as the widely-used logging tool Log4j would be deemed to be violating their terms and privacy policies.

It has served as a clear warning that

SUMMARY

- ***As cyber risks*** continue to ramp up, stricter regulations and laws are following suit.
- ***Several new pieces*** of legislation have been crafted on global, federal and state levels.
- ***These new cyber*** regulations are meant to prioritize consumer loss while also giving power back to both federal and state agencies.

With our deep product and industry expertise spanning more than 20 specialized segments, we deliver global solutions to address the unique risks you face, wherever you operate. Our experts have a comprehensive understanding of your entertainment business. Let us tailor a solution for your specialized insurance needs.

To learn more, talk to your broker or visit intactspecialty.com

intact INSURANCE specialty solutions

the FTC is prepared to exercise its rights and pursue offenders.

INCREASING AGENCY POWERS

At the state level, California has led the way on data privacy with the California Privacy Rights Act (CPRA), which comes into force on January 1, 2023.

The CPRA builds on the California Consumer Privacy Act, which was signed into law in June 2018, with the establishment of the California Privacy Protection Agency with its own regulatory investigative and enforcement powers.

"Increasingly, federal agencies such as the SEC and FTC are taking a more active role in cybersecurity enforcement," said Mary Hildebrand, partner at Lowenstein Sandler.

"That's now being extended to individual states, such as California setting up its own dedicated enforcement agency."

Nevada amended its privacy law in June 2021 to include its own modified version of the CCPA's "Do Not Sell My Personal Information" requirement. This obliges businesses to have a clear and conspicuous webpage enabling consumers to opt-out of having their data sold to third parties.

Other bills are set to follow suit, with the Virginia Consumer Data Protection Act being passed on January 1, 2023 and the Colorado Privacy Act on July 1, 2023. Utah is also awaiting the governor's signature on its new law, set for December 31, 2023.

"Increasingly, federal agencies such as the SEC and FTC are taking a more active role in cybersecurity enforcement. That's now being extended to individual states, such as California setting up its own dedicated enforcement agency."

***— Mary Hildebrand**, partner, Lowenstein Sandler*

The General Data Protection Regulation, introduced in May 2018, remains the most significant data protection law in Europe and UK, with several cases having already been brought against companies in recent months.

Then there's the EU-U.S. Data Transfer Pact, which has been agreed to in principle, enabling entities to transfer data between the two regions.

Brazil also enacted its own General Personal Data Protection Law in September 2020, which restricts data transfer, while China did likewise with its Personal Information Protection Law in November 2021, intended to manage data flow out of the country.

However, the introduction of India's new data protection law has been delayed by the COVID-19 pandemic.

"One thing is for certain, strengthening cybersecurity practices and consumer rights to privacy and control over their personal data are here to stay," said Gamelah Palagonia, executive vice president, cyber development and regulatory leader at Willis Towers Watson.

"Since the enactment of the EU's GDPR, other countries have brought in their own regulations and more are expected to follow in their footsteps."

RULE OF ONE FOR MANY

To come to grips with the new regulations, senior management needs to work with its general counsel and legal team to map out and understand all the different laws and how they will affect their business. Given that much of the legislation is broadly similar, particularly at the state level, if they follow one law, they can then expand upon that to comply with the regulations in other jurisdictions.

"A possible path is to build your approach to the most restrictive standard so that you are compliant across all the jurisdictions in which your business operates; it makes administration a lot easier because if you're compliant to the highest standard, then you clearly meet all the lower thresholds," said Mehvish Femia, chief legal officer at Resilience.

"It also makes your operations run smoother, because there's only one process to follow, rather than 50 — and when you have changes, you're only changing one regime."

Many regulators will also require firms to have a robust incident response and recovery plan that can be rapidly deployed in the event of an incident and is regularly tested. Risk managers also need to keep on top of changes in data privacy law and how data is being used.

"Risk managers must stay informed on any changes in the collection, use, transfer and retention of personal information," said Elizabeth Shirley, co-chair of the cybersecurity and data privacy team at Burr & Forman.

"They should know what personal information is collected, where it is stored, what is the purpose of collecting it, who has access to it, how long it is retained and is any unnecessary personal information collected."

It's also key to carry out due diligence on third-party vendors and service providers to make sure that they comply with these new regulations. Similarly, employees need to be regularly trained on the latest cybersecurity practices, given that they are one of the biggest causes of data breaches.

Companies also need to ensure they have cyber insurance in place to provide defense against regulatory actions and associated fines and penalties following a data breach, where they are insurable by law. They must also understand the coverage terms to avoid potential claim denials. **&**

ALEX WRIGHT is a UK-based business journalist who previously was deputy business editor at The Royal Gazette in Bermuda. You can reach him at riskletters@theinstitutes.org.

The California Privacy Rights Act

Hailed as one of the most significant pieces of data privacy legislation, the California Privacy Rights Act (CPRA) comes into effect on January 1, 2023.

As an amendment to the California Consumer Privacy Act (CCPA), it includes additional privacy protection for consumers.

Despite coming into effect next year it will retroactively apply from January 1, 2022 onwards.

All businesses, except the public sector, non-profit organizations and entities covered by the Health Insurance Portability and Accountability Act will have to comply with the new regulation which governs companies that process or sell California residents' personal information, including service providers, third-parties and contractors.

It affords consumers the following rights:

- The right to know personal information collected by the business about the consumer, from whom and why it was collected and, if sold, to whom;
- The right to delete personal information collected from the consumer;
- The right to opt-out of the sales of personal information;
- The right to opt-in to the sale of personal information of consumers under the age of 16;
- The right to non-discriminatory treatment for exercising any rights;
- And the right to initiate a private case of action for data breaches

As well as two new rights:

- The right to correct inaccurate personal information;
- And the right to limit use and disclosure of sensitive personal information

The CPRA is also the only State law that grants consumers a private right of action for security breach violations.

"The CCPA/CPRA is most impactful for two primary reasons," said Gamelah Palagonia, executive vice present, cyber development and regulatory leader at Willis Towers Watson.

"First, it imposes new business obligations representing operational changes. For example, businesses must provide notice of consumer rights, honor consumer rights, fulfill disclosure and data retention obligations, facilitate consumer requests and implement security safeguards."