April, 2018

This Month's Top Issues

In the field of international trade, the growing potential for damage from data breaches for consumers, shareholders and markets alike is on authorities' minds. As a result, they are using the tools at their disposal to encourage or mandate that businesses maintain higher cybersecurity standards. What follows is a roundup and analysis of key data security issues making headlines, and what cybersecurity professionals should know.

EU, China Set Global Bar on Data Privacy

In January, China released the final draft of its new data privacy standard, adding to the country's growing body of cybersecurity law. With the EU's General Data Protection Regulation, from which the Chinese Personal Information Security Specification took inspiration, the enactment suggests an emerging global standard for data privacy.

The Chinese and European frameworks both go into effect in May 2018. They share some common ground, giving data portability and erasure rights to individuals and aligning the definitions of personal information.

But where the GDPR is a comprehensive regulation, the Chinese standard is just one part of the country's broader cybersecurity picture—and, unlike the GDPR, the standard is technically voluntary. Nonetheless, regulators are expected to refer to the standard during audits, and noncompliance could well guide enforcement.

One substantive difference is in the treatment of consent. In this respect, Samm Sacks, senior fellow at the Center for Strategic and International Studies, a bipartisan think tank, said the Chinese definition "is something less than explicit consent as defined in the GDPR." The Chinese standard requires affirmative consent where sensitive personal data is concerned, but departs from the European regulation in other circumstances where implied consent may reasonably be interpreted to suffice, although this is not specifically laid out in the text.

The result is that the definition of consent "in some cases, may be more permissive," Sacks said. Her own analysis concludes the standard is intended to be somewhat less restrictive than the GDPR to avoid hampering the growth of industries like artificial intelligence, which are seen as critical to China's economic potential.

In comparison, the U.S. has no overarching approach to data privacy. It is instead handled either in a sector-specific way, as with health care privacy, or under the Federal Trade Commission's mandate or, in some cases, at the state level. With important trade markets like Asia and the EU taking the first-movers' advantage, the U.S. is relegated to a reactive position, Sacks said.

"As a result, U.S. companies are having to come up with very elaborate, complex arrangements to deal with emerging data policies in the EU and China," she said. "It creates a difficult situation for U.S. companies operating in a multinational context." The result is that as the global conversation about data privacy develops, it is one from which the U.S. is largely absent.

The Takeaway: China and the EU are taking the lead in shaping the conversation on global data privacy standards. Although nominally voluntary, the Personal Information Security Specification still warrants close attention to compliance guidance by businesses subject to existing Chinese cybersecurity law.

CRYPTOJACKING ON THE RISE

Cloud security company RedLock reported in February that Tesla was the latest victim of a new kind of cyberattack on the rise since late last year: cryptojacking. These attacks are less about accessing proprietary data than illicitly co-opting processing power to mine cryptocurrency. Most targets aren't as high profile as Tesla, but more typically everyday website visitors who unwittingly visit pages where their browsers are surreptitiously hijacked to mine coins in the background. The website Whorunscoinhive.com estimates more than a billion users monthly are already being cryptojacked.

SEC Urges Improved Cybersecurity Risk Disclosure

In response to the rising frequency and damage of data breaches on publicly traded companies, the Securities and Exchange Commission in February updated its guidance on cybersecurity disclosures. Critics—including from within the agency's ranks—say the guidance does not go far enough.

The Cybersecurity Interpretive Guidance is intended to "reinforce and expand" upon the SEC's previous 2011 guidance, explicitly highlighting the need for disclosing cybersecurity risks and adopting internal procedures to control such risks. It also reiterates prohibitions on insider trading based on unpublicized cybersecurity incidents.

"It puts boards of directors on notice about the important role they have to play, particularly when it comes to cybersecurity risk management," said Paul Rosen, former federal prosecutor and partner in Crowell & Moring's white-collar regulatory enforcement, cybersecurity and data privacy group, in an emailed response.

SEC Chairman Jay Clayton said in his official statement the guidance would promote "clearer and more robust disclosure," but others on the commission disagreed. Noting in her statement that the 2011 guidance did not result in an increase of useful disclosures for investors, Commissioner Kara Stein lamented this "more or less reissued" version as inadequate.

Stein outlined several ways in which the agency could have done more, including incorporating actionable suggestions from advisory committees and academics to improve disclosure usefulness for investors. She was joined in her reserved support by Commissioner Robert Jackson, who, in his statement, said the guidance "essentially reiterates years-old staff-level views on this issue."

This latest guidance comes as high-profile cyberattacks are on the rise and, as Bloomberg Law notes, securities fraud class-action lawsuits are increasingly being brought by shareholders. "Plaintiffs' lawsuits are likely to continue so long as cybersecurity incidents occur, and consumers and investors are harmed," Rosen said.

"The viability of these suits will largely depend on whether and to what extent courts determine that there has in fact been an injury to consumers and investors bringing these actions." The trend further underscores the need for robust cybersecurity risk and policy disclosures before breaches occur.

The Takeaway: Whatever the shortcomings of the latest SEC guidance, it highlights a growing focus on the responsibility of public companies to adequately prepare investors for cybersecurity risks and beef up internal policies. Combined with the guidance, a rise in securities fraud class actions in the wake of data breaches should emphasize the need for improved cybersecurity risk disclosures.

APEC Privacy Certification Aims to Boost Trust

Earlier this year, the U.S. became the first Asia-Pacific Economic Cooperation member to sign on to a voluntary program certifying data processors for compliance with shared privacy principles. Singapore followed suit in March. The program is intended to boost trust and cooperation between data processors and controllers, as well as enhance the marketability of certified processors among APEC markets.

The Privacy Recognition for Processors program rounds out APEC's approach to consumer data, complementing the existing Cross-Border Privacy Rules and Privacy Framework principles. According to the U.S. International Trade Administration blog, voluntary PRP participation requires that processors self-certify compliance with baseline security and accountability standards before submitting to audit by an APEC accountability agent. In addition, processors should be able to demonstrate complaint handling procedures and undergo ongoing monitoring and periodic recertification.

The program is designed to enhance cooperation between processors and data controllers, which are not required to contract with PRP-recognized processors. Doing so, however, would provide assurance the processor had been vetted for appropriate security controls under the CBPR.

Small- and mid-size businesses may find further benefit in PRP certification where they do not have in-house resources or knowledge for comprehensive privacy overhaul, said Markus B. Heyder, vice president and senior policy counselor at the privacy and security-focused Centre for Information Policy Leadership, in an emailed response. "Going through the PRP certification process with a third-party APEC 'Accountability Agent' will provide the outside expertise together with the assurance that they are doing it correctly," he said.

Certification may prove to be straightforward for processors already preparing to comply with other data privacy frameworks, such as the EU's General Data Protection Regulation. For multinationals undertaking steps toward GDPR compliance, Yodi S. Hailemariam, a cross-border information governance lawyer at Drinker Biddle in

Cybercrime by the Numbers:

130 Average number of security breaches each year

27.4% Increase in average annual number of security breaches

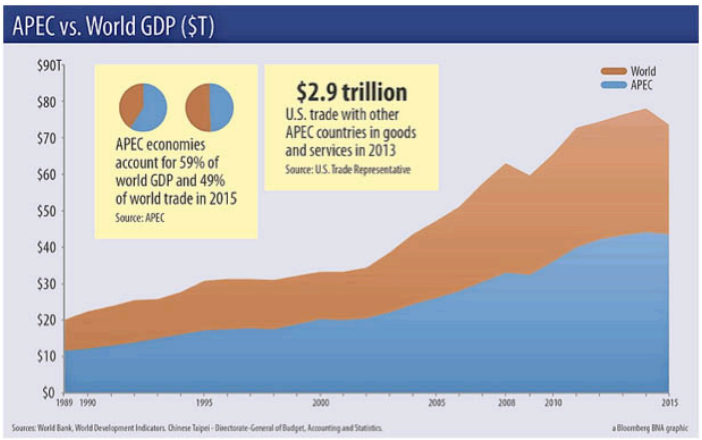
$11.7 million Average annualized cost of cybersecurity

$6 trillion Estimated cost of cybercrime, annually, by 2021

Washington, D.C., said she doesn't see the PRP being more onerous than what they are likely already doing.

She said the PRP fits "perfectly well" within the broader picture of emerging data privacy standards. "It's an illustration of the global trend towards heightened regulation and focus on protecting private citizens' data," Hailemariam said. "I think we're seeing a very clear overall trend towards taking personal data very seriously and companies taking appropriate steps to do so."

The Takeaway: The PRP is another facet of the emerging global data privacy landscape and certification validates that basic data protections are being adhered to, allowing participants to distinguish themselves from competitors in APEC markets.



Conclusion

A consensus on global data privacy is beginning to emerge as new frameworks come into force around the world, meaning businesses with global aspirations will sooner or later need to comply to protect their access to foreign markets. Even those with a solely domestic focus may find it beneficial to adhere to higher standards than suffer public and shareholder fallout from breaches.

About (ISC)²

(ISC)² is an international nonprofit membership association best known for its award-winning Certified Information Systems Security Professional (CISSP®) certification, with additional certification and education programs that holistically address security. Our membership, 130,000 strong internationally, is made up of sought-after cyber, information, software and infrastructure security professionals who are making a difference and helping to advance this new industry. Our vision to inspire a safe and secure cyber world reaches the general public through a commitment to social responsibility via our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit http://www.isc2.org, follow us on Twitter or connect with us on Facebook.