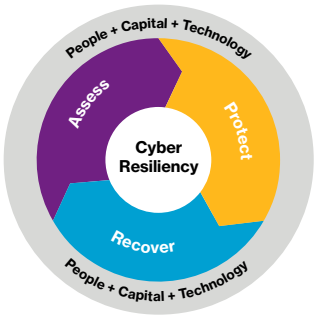

Decode protected.

Could organizations deemed 'too big to breach' face more stringent cyber regulations?

by **James Bobotek, Esq., Aaron Coombs, Esq., Dan Twersky**

After numerous high-profile cybersecurity failures in 2017, regulators in the U.S. and E.U. are considering stricter regulations for organizations that are deemed too critical to a nation's infrastructure to breach. The rules would be similar to those enacted in the U.S. following the 2008 financial crisis, after which certain financial institutions were designated as "too big to fail" under the Dodd-Frank Act, and subject to stricter regulations.

Similar measures could be enacted in relation to cybersecurity. Two primary questions arise:

- Are there organizations that are "too big to breach," i.e., too critical to U.S. infrastructure or hold too much sensitive personal information?
- If so, what sort of regulation for these companies is feasible?

While only 10% of the 2017 Reported Claims Index involved coverage for privacy and/or security-related regulatory investigations or proceedings, a number of recent incidents have raised awareness and brought calls for heightened regulation and oversight. From the malware and ransomware attacks that have left entire organizations crippled for days, to theft of data from political parties, to the recent catastrophic breaches (in both numbers and severity) of companies that have exposed millions of individuals' personal data, companies can no longer assume cyber threats won't apply to them.

While the U.S. government may not be in a position to "bail out" institutions that suffer the consequences of a major data breach, it may heed the call to proactively prevent such breaches by imposing increased regulatory scrutiny on them. As we are beginning to see with some state legislation, it may also protect companies from liability arising from data breaches if the companies in question have taken steps to align their cybersecurity programs with industry standards.

Early strides in cyber regulation

Cybersecurity regulation and oversight in the U.S., while making strides, remains fragmented. There is a wide array of data privacy and cybersecurity regulations enforceable on both the state and federal levels, yet there is no overarching body responsible for cybersecurity coordination among states. In addition, there is a patchwork of voluntary guidelines, recommendations and best practices circulating, but as history has shown, these may not be enough.

In many respects, there are already a number of institutions that have been deemed too important to suffer a data breach and are therefore already subject to additional regulation. These include:

- Power companies under the jurisdiction of the Federal Energy Regulatory Commission subject to increased cybersecurity compliance requirements
- Health care institutions with protected health care data subject to the requirements of the Hi-Tech Act and the Health Insurance Portability and Accountability Act (HIPAA)
- Federal agencies subject to the Federal Information Security Management Act of 2002

Recently, other sectors have fallen under closer scrutiny as well, in the U.S. and abroad:

- In March 2017, financial services companies operating in New York became subject to mandatory and enforceable cybersecurity requirements; other companies in Colorado are subject to similar regulation.
- In October 2017, the National Association of Insurance Commissioners passed a model data security law which, if fully enacted, would require insurance companies to implement information security programs, conduct risk assessments, develop incident response plans, and comply with certain investigation and notification requirements in the event of a breach.
- Last year, the European Parliament passed the Network and Information Security (NIS) directive in relation to cybersecurity and critical infrastructure. Operators within industries earmarked as critical by individual member states — including energy, health, banking, public water and digital services — have to be certified to meet common E.U.-wide cybersecurity standards. NIS also instituted reporting requirements for organizations faced with a security incident.

Defining "too big" in the context of data breaches

Major companies that fall within the 16 critical infrastructure sectors already identified by the Department of Homeland Security as "so vital to the United States that their incapacitation or destruction would have a debilitating effect" on national security and the economy are likely candidates to be declared "too big to breach." Industries involving nuclear reactors or public water systems might easily fall into this category. Additionally, cybersecurity regulations such as the Critical Infrastructure Protection standards that apply to operators of the electric grid could be replicated for other industries, as they have already been expanded to apply to the supply chains of these operators.

In others sectors, however, defining "too big" or "critical" is more difficult.

One method for identifying such companies would be to simply set a threshold based on the number of individual records containing protected personal information that could potentially be breached. For example, companies with vast troves of personal information could be targets of increased regulatory scrutiny.

It's worthwhile to note that opponents of this approach are likely to assert that it would stifle companies in the data monetization business, which in turn might have a substantial impact on e-innovation. Further, setting such a threshold could incentivize companies to minimize the amount of personal data they maintain by either collecting less information in the first place or permanently destroying information they no longer need. In addition, defining, identifying, quantifying and verifying whether a company exceeded such a threshold would be difficult.

In lieu of such a threshold, another option could be a broadly applicable law or regulation under which the penalties for noncompliance are indexed to a clearer metric, such as annual sales or revenue. Such a law could be modeled after the E.U.'s General Data Protection Regulation — whereby penalties for noncompliance vary based on the company's worldwide turnover (i.e., upwards of 4% of worldwide turnover or €20 million, whichever is higher, would trigger the penalty).

It should come as little surprise that some have called for the three major U.S. credit reporting bureaus to be treated more like public utilities and therefore subject to increased oversight by a government regulator, as their primary customers are banks, insurance companies and other commercial entities — not the consumers whose data is collected.

Regulation and enforcement for cyber crimes

Because technology is ever evolving and threats are ever changing, any "too big to breach" regime would need to focus more on processes and procedural requirements, rather than on specific technology standards. One source that lawmakers might turn to for precedent is the National Institute of Standards and Technology (NIST).

NIST has been at the forefront of cybersecurity protocols and is now involved in almost every aspect of federal government IT standards. In particular, the H.R. 1224 NIST Cybersecurity Framework, Assessment, and Auditing Act, undergoing revision at the time of this writing, would expand NIST's role from a neutral advisor that develops best practices to a quasi-enforcement role involving the auditing of federal agencies.

The NIST Cybersecurity Framework consists of five core cybersecurity functions that are common to any organization: identify, protect, detect, respond and recover. Within each function, supporting categories and subcategories further define the activities that can be implemented. Any "too big to breach" law — like many existing or proposed cybersecurity laws — would likely incorporate many of these same concepts established by NIST.

We are already beginning to see government agencies use their civil enforcement powers to fine companies for lacking in data security protocols. Given the Federal Trade Commission's strong commitment to protecting consumer data, such enforcement is only likely to increase. A number of companies have been fined this year on data security grounds.

While fines are one enforcement mechanism, class-action lawsuits are also emerging. In August, the D.C. Court of Appeals ruled that a class-action lawsuit against a health care organization involving a data breach of nearly 1.1 million records could move forward. This overturned the District Court's ruling, which found that plaintiffs had not suffered actual harm. The Supreme Court was petitioned to hear the case, a worrying precedent to companies who are not taking every action to protect the privacy of their customers.

Increased compliance could also come in the form of a carrot instead of a stick. Proposed Ohio legislation aims to be the first of its kind in the U.S., offering "legal safe harbor" to entities that have implemented industry standards on cybersecurity. This could be used as an affirmative defense to a cause of action in state data breach cases. The bill relies on the NIST Cybersecurity Framework as the industry standard. As discussed earlier, commentators have pointed to this bill as an important incentive for businesses to voluntarily maintain compliance to such standards.

One of the most important areas for regulation is around information sharing. The E.U.'s General Data Protection Regulation (GDPR), discussed earlier, requires data breach notification within 72 hours of becoming aware of an incident. This law is extraterritorial in reach and will likely impact many U.S. companies. Congress could follow suit, as on December 1, 2017, several senators introduced a Data Security and Breach Notification Act which, if passed, would require notification to law enforcement within 10 days of discovery. Individuals who knowingly conceal a data breach could face up to five years in prison.

In addition, this summer, the Department of Health and Human Services (HHS) Health Care Industry Cybersecurity (HCIC) Task Force released their report detailing risks and recommendations for improving security in that sector. Improving information sharing was one of their six "imperatives." To do so, they recommend broadening the scope of Information Sharing and Analysis Organizations (ISAOs) and working more closely with the Department of Homeland Security's National Cybersecurity and Communications Integration Center. Similar information sharing requirements could be included in a "too big to breach" law.

Currently, many of the organizations that could be deemed "too big to breach" may already be implementing some of these actions, but face a multitude of state laws and regulations in the event of an incident. Thus, some may welcome a preemptive federal cybersecurity law, even if it mandates practices that are now just voluntary.

The role of insurance in cyber protection

How would insurance coverage play a role in a "too big to breach" scenario? First, some companies could legally be required to purchase cyberinsurance – just as hazardous waste facility owners and operators are subject to financial assurance requirements to comply with EPA regulations. Second, insurance underwriters play an indirect and largely unintentional enforcement role themselves by helping organizations develop risk mitigation strategies. They also identify and reward best practices through favorable terms and reduced premiums for companies with "best-in-class" risk profiles.

As underwriters continue to expand their scope, the cultures around employee engagement, cyber awareness and related training is becoming a more integral part of many organizations' due diligence process. A regulator investigating an organization following a cyber event may take into consideration a positive culture and steps taken to mitigate harm when assessing damage and determining penalty.

Finally, insurance could be used as a hedge against the costs of an investigation or enforcement action, as cyber policies typically provide coverage for fines assessed in connection with the violation of a privacy regulation. It is also reasonable to expect further regulatory innovation from the cyberinsurance industry to meet changing risks in the near future, as new threats are uncovered and cyber awareness grows.

James Bobotek is a Partner in the Litigation Group of Pillsbury Winthrop Shaw Pittman LLP, practicing in its Washington, DC and Northern Virginia offices.

Aaron Coombs is Special Counsel in the Insurance Recovery Group of Pillsbury Winthrop Shaw Pittman LLP, and practices in its Washington, DC office.

Dan Twersky, is a Willis Towers Watson claim advocate and cyber claim leader based in New York City.

Contact

Dan Twersky
Willis Towers Watson
212 915 8580
dan.twersky@willistowerswatson.com

James Bobotek, Esq.
Pillsbury Winthrop Shaw Pittman LLP
703 770 7930
james.bobotek@pillsburylaw.com

Aaron Coombs, Esq.
Pillsbury Winthrop Shaw Pittman LLP
202 663 8071
aaron.coombs@pillsburylaw.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson