Perspective: What Will Be the Defining Cybersecurity Issues In 2016?

1/19/2016 by Margaret Loveman, Alexander Major, Craig Newman, Philip R. Stein, Tom Vincent, II | JD Supra Perspectives

Like 0 G+1 1 Tweet Share 6

> *2016 will be another important year in cybersecurity and data privacy, with regulators and the courts continuing to confront difficult issues – many of which involve laws enacted decades before today's Internet, decades before cloud computing and long before huge amounts of data were stored in servers around the globe* - **Craig A. Newman**, partner at Patterson Belknap Webb & Tyler

As data breaches and their related obligations and liability risks continue to pile up with every passing year, we asked attorneys writing on JD Supra to answer the question: **What will be among the defining issues for cybersecurity in 2016?**

Here is what we heard back:

1. Testing the Limits Of What's Covered By Cybersecurity Insurance

Philip R. Stein, attorney at Bilzin Sumberg Baena Price & Axelrod: "A defining cybersecurity issue in 2016 will be litigation over what data breaches, and related losses, are really covered by cybersecurity insurance, and by other types of insurance. Do cybersecurity insurance policies cover physical property damage that may result from a cyberbreach compromising a company's logistics or supply chain? Does a directors and officers' policy cover a data breach-related shareholder derivative suit? What kind of security vulnerabilities might fall within exclusions to coverage for an insured?

Though the answers to some of these questions will of course hinge on case-specific policy language, broader legal principles and precedents also still need to be more fully developed. More generally, the rights and obligations of various types of financial services providers - not only insurers, but banks and credit card companies - in the aftermath of data breaches will likely be front and center in the world of cybersecurity and data privacy litigation in the coming year."

...broader legal principles and precedents also still need to be more fully developed.

Margaret Loveman, attorney at Butler Snow: "Insurance coverage makes the world of business litigation go 'round. For several years, whether general CGL insurance coverage is triggered in the event of a data breach - and the extent of that coverage - has been a topic of debate. In 2016, we should see that debate continue. In a typical CGL form, 'personal and advertising injury' is defined, in part, as injury, including consequential 'bodily injury' arising out of oral or written publication, in any manner, of material that violates a person's right of privacy. For years, litigators on both sides have

argued about whether publication of a customer's private information by a third party, such as a hacker, is sufficient to trigger coverage.

In 2015, many were looking to *Zurich Am. Ins. Co., et al. v. Sony Corp. of Am., et al.*, Index No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014), to help settle the question. Unfortunately, the parties settled in April 2015 prior to the appellate court's opinion. Because a ruling on this issue will have a significant impact on coverage issues, expect to see other attempts to settle this issue in 2016."

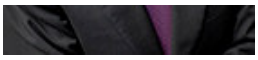
2. The 'Rise of the Regulators'

Alexander Major, associate at Sheppard Mullin: "In the world of cybersecurity, I am sure that 2016 will be viewed as the 'Rise of the Regulators.' The FTC has already seized a firm foothold in that world, the FCC is becoming an increasing visitor to it, and the SEC has been poking around – but in 2016, I think we'll see a huge amount of 'growth' in the enforcement of 'regulations' driven by agency OIGs. The reason for this is simple: Companies now 'know better' (or, in the eyes of the regulators, they should know better). In February 2014, the National Institute for Standards Technology (NIST) promulgated its 'cybersecurity framework,' which provided a flexible list of standards, best practices, and guidelines intended to help address various cybercrime risks. More recently, in June 2015, NIST published Special Publication 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,' guidance for federal agencies to ensure that sensitive information remains confidential when stored outside of federal systems, (that is, how data should be protected by commercial companies). In this regard, I would suggest that, while NIS TSP 800-171 may not be directly or expressly applicable to all commercial companies, there is now an emerging 'standard' by which a commercial company's cybersecurity reasonableness can be measured by the federal regulators.

When addressing a data breach, I suspect federal regulators, each of whose agencies is beholden to NIST special publications, are likely to find SP 800-171 to be a comfortable 'fall back' position when asked to assess the reasonableness of a company's security efforts. What's more, one cannot forget that the new DoD cybersecurity regulations (e.g., 48 CFR Subparts 204.73, 252.204–7012, and 32 CFR § 236) require specific security controls be in place for certain defense contractors handling critical defense information. The DoD and its auditors have been relatively quiet as they, presumably, try to better understand what is actually required under their new rules. But I suspect that by the end of 2016, we will have experienced our first full-blown DoD incursion into the slippery world of cyber regulation. But with the ability to choose from between the risks of fraud/false certification, suspension and debarment, or breach of contract, the final guise of DOD's eventual 'enforcement' regime is anyone's guess. The bottom line is that commercial companies need to be prepared to address the five main cyber risks: (1) hackers, (2) insiders, (3) insurance providers, (4) plaintiffs, and (5) government regulators. For 2016, failure to do so may mean a knock at the door that you're not really expecting."

Key areas to watch include developments at the Federal Trade Commission and precisely where the bar sits for the commission to commence an enforcement action.

Craig A. Newman, partner at Patterson Belknap Webb & Tyler and chair of the firm's Privacy and Data Security practice group: "Not surprisingly, 2016 will be another important year in cybersecurity and data privacy, with regulators and the courts continuing to confront difficult issues – many of which



involve laws enacted decades before today's Internet, decades before cloud computing and long before huge amounts of data were stored in servers around the globe. Key areas to watch include developments at the Federal Trade Commission and precisely where the bar sits for the commission to commence an enforcement action. Does the agency need to show an actual injury or just a threat of one? The answer to that question will likely be addressed in the agency's long-running dispute with LabMD. Closely related is the standing issue in civil data breach cases and what showing a breach victim must make to sustain a lawsuit when an individual's information has been compromised. The Spokeo case pending before the Supreme Court should answer at least part of that question. It's also likely that we will see an increase in shareholder derivative litigation arising out of data breaches – especially against companies that have suffered multiple breaches. And finally, the Second Circuit's decision in U.S. v. Microsoft, otherwise known as the Dublin server case, will have broad implications for U.S. companies that store data beyond U.S. borders, for Internet privacy and international relations. However decided, the Second Circuit is likely to be a pit stop in the case – either on the way to Congress or the Supreme Court."

3. With Rising Use of Mobile Devices, Continued Conflict Between Corporate and Personal Interests

Tom C. Vincent II, attorney at GableGotwals and a former bank compliance officer: "Much like the common expression 'All politics is local,' increasingly we similarly see that 'All cybersecurity is local' – local (mobile) devices, that is. As more and more individuals utilize mobile devices for critical business functions – whether provided by their employers or (more commonly) purchased individually – more and more critical business information leaves the protection of organized information security departments for the inconsistent vigilance of these individual users. While remote wiping of personal devices continues to be relied upon as one (if not the only) corporate protective action, employees continue to chafe at the

perceived priority given to corporate interests over their own with respect to information on their own devices.

Revisions to the Fair Labor Standards Act increasing the number of employees eligible for overtime may reduce the overall population of personal devices accessing corporate information; many companies, however, may be unable to make such adjustments to their business processes. As a result, those companies will be forced to maximize the non-overtime hours of their employees and increasingly rely on mobile devices (and the corresponding risk) to squeeze additional productivity out of a shorter (i.e., 40-hour) workweek. This increased risk of breaches resulting from personal devices may well be exacerbated as hackers pay more attention to non-personal (i.e., corporate) information. As with banking, when the passage of the Bank Secrecy Act and adoption of related controls pushed illegitimate financial activity into new channels (e.g., trust departments and broker-dealers), increased protection of personal information may result in corporate information becoming a more frequent target of attack.

...we may very well see more companies return to the 'company-owned device' model as a business practice.

The value of such non-personal information was seen last year, as the Securities and Exchange Commission brought action against defendants who were able to generate more than $100 million in illegal trading profits from such information. If we move closer to a national breach notification law – but one that may still focus on personal information – this type of information will only become more valuable as it becomes comparatively less protected. As these issues ultimately converge, we may very well see more companies return to the 'company-owned device' model as a business practice, or more workers push for it as an employee concern – each wanting greater protection of their own information from actions of the other."

*