Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity & Privacy Predictions For 2018

By **Allison Grande**

Law360, New York (January 1, 2018, 3:04 PM EST) -- Some of the biggest privacy and cybersecurity buzzwords from the past year will only continue to grow in prominence in 2018, with attorneys predicting a further expansion of an already complex data breach landscape, greater attention being paid to internet-connected devices, and even more additions to an already vast global patchwork of laws.

Here, cybersecurity and privacy attorneys identify some major trends and offer predictions for what practitioners should expect to hear from their clients in the coming year.

Data Breach Threats Will Get Bigger, Badder

After a year marked by global ransomware attacks that temporarily took down major businesses and a massive data breach at Equifax that compromised personal data of nearly half of the U.S. population, attorneys are expecting the cyberthreat environment to only keep growing and evolving in the new year.

"In the data breach world, every year we ask, 'Are we done, is this the biggest and baddest it's going to be?'" said Squire Patton Boggs LLP privacy and cybersecurity group co-chair Robin Campbell. "I think it's safe to say that the answer is no. Equifax showed us that and demonstrated that no one is safe."

Jim Halpert, co-chair of DLA Piper's global data protection, privacy and security practice, said he expected the now well-known cyber arms race to only escalate in the coming year, with hackers constantly looking for new attack methods and those who are charged with protecting systems striving to "up their games."

"The cyberthreat is constantly changing, and that leads to worse incidents, and that's just been a constant every year," Halpert added.

Attorneys are gearing up for more of the same on the cyber front in 2018, while watching out for new potential twists. They predict ransomware attacks that hold networks hostage until a sum of money is paid will only grow more sophisticated, while social engineering attacks that trick employees and other computer users into clicking on infected links will also continue.

"Most of the companies I work with have ransomware plans and capabilities in place now and are

moving to establish the kind of resources they need to be able to operate in advance of a ransomware attack," said Hogan Lovells partner Harriet Pearson. "That doesn't mean they have all the answers — the bad guys and gals are still smart, and these attacks will still be pervasive. But the good side is that most companies are developing their capabilities to stop them from getting in."

With companies focused on the biggest attack methods of recent months, attorneys worry about other avenues that have yet to be widely exploited. Lisa Sotto, head of Hunton & Williams LLP's privacy and data security practice, said she's concerned in particular about data integrity issues.

"We haven't seen what could be a cataclysmic event with respect to data integrity and the changing of data," Sotto said. "It's not hard to imagine the havoc that could be wrought if the levels are changed at a wastewater treatment plant or data is changed at a hospital. The ransomware actors have perfected their trade, and now they can move on to more damaging exploits. We're likely to see more audacious attacks, since the audacity levels of attackers have reached stunning new levels."

As companies focus more on the protection of personal data, hackers are likely to set their sights on other types of business information, and several attorneys tagged critical infrastructure as an area that may be particularly vulnerable in the coming months.

"Three years ago, we were preaching about ransomware, and now we're in the ransomware age," said Squire Patton Boggs partner Tara Swaminatha. "The next group of attacks that will likely happen over the next few years may be malicious actors not trying to steal information, but sabotaging companies and changing things."

Stuart D. Levi, the head of Skadden Arps Slate Meagher & Flom LLP's privacy and cybersecurity group, noted that critical infrastructure companies are "in a state of heightened awareness" about their cybersecurity risks and are taking steps to protect themselves.

"The question will be whether those measures are good enough or not," Levi added.

Across a wide range of industry sectors, companies are stepping up their cybersecurity protections, and attorneys only expect security measures to continue to improve and evolve with the hackers, with a particular focus on employee training, patching systems more quickly and conducting more thorough data assessments and security audits.

"There's going to be more breaches for sure, so from a preventive standpoint, we're going to keep telling clients that proper security measures, programs and plans are key," Greenberg Traurig LLP partner Francoise Gilbert said. "I've been working on data breaches since 1991, and while companies are becoming more aware, these breaches will keep happening if companies don't do what they need to be doing."

Campbell noted that as attacks become more widespread, companies are likely to shift their focus from questioning how such an incident could happen to instead honing in on the quality of their incident response, while Shook Hardy & Bacon LLP data security and privacy group chair Al Saikali observed that he's noticing larger companies undertaking more sophisticated information security assessments.

"Where a few years ago the goal was to determine whether they were meeting or exceeding industry standards, they are now engaging in red teaming exercises, hiring security experts to break into their system to identify potential vulnerabilities," Saikali added.

Pressure is likely to mount from all sides for companies to dedicate even more time and resources to these vulnerabilities in the coming year, with Foley & Lardner LLP partner Michael Overly predicting that we will continue to see a movement by the Trump administration to tighten up information security requirements for government agencies, which "by virtue of that move will flow down to private entities."

Lawmakers will also keep devoting attention to this area, with at least one recent federal legislative proposal floating the idea of criminal liability for such hacks, and companies will additionally need to contend with the usual influx of consumer and shareholder class actions that typically follow such high-profile incidents, meaning that it will be imperative to ensure that more than just the IT departments are still keeping close track of these issues, attorneys noted.

"Boards of directors will continue to be interested in hearing about privacy and data security developments as well as developments involving emerging technology, artificial intelligence and big data," said VLP Law Group LLP partner Melissa Krasnow.

Companies may also soon have to grapple with a new legal risk from state and local governments, attorneys noted. The city of San Francisco and the Massachusetts attorney general sued Equifax, while Chicago went after both the credit reporting giant and Uber following the disclosure of their data breaches, and experts say watching how these suits unfold in 2018 will be key.

"Next year, keep an eye on out for cities and states as they start enforcing their state privacy and consumer protection laws against defendants who fail to secure their customers' data," said Jay Edelson, the founder of plaintiffs firm Edelson PC.

Kaufman Dolowich & Voluck LLP partner Tad Devlin added that the newest lawsuits are notable in that they signal a larger trend of state regulators being more focused on enforcement and regulation in the privacy and data security sphere.

"We're seeing regulators clamping down in terms of the data security measures that need to be put in place by companies, and we're seeing more layers of regulations and divisions in enforcement," Devlin said.

Internet of Things Will Spark New Security Risks

The rise of home appliances, medical devices, automobiles and other consumer products connected to the internet, commonly known as the internet of things, was a major talking point in 2017, and attorneys anticipate that the IoT — and its inherent privacy and security risks — will continue to be the talk of the town in the new year.

"Everything is 'smart' these days — it's so rare that any device is going to hit the market that doesn't offer some kind of internet-connected component," said Emily Tabatabai, a founding member of the cybersecurity and data privacy team at Orrick Herrington & Sutcliffe LLP. "These products bring with them a whole host of privacy and data security issues that have not been pretty well addressed so far, so it will be interesting to see how regulators respond and the possibility of cyber incidents and litigation coming with respect to these products in 2018."

An important shift in the upcoming year will likely be companies that manufacture these devices

becoming more aware of the privacy and security risks they may pose, according to attorneys.

"There's been a lot of talk lately about privacy by design, but now there's likely to be more discussion about security by design," said Tony Scott, a Squire Patton Boggs senior adviser and former federal chief information officer for the U.S. government. "The tendency has been to duck tape and bubble wrap around older technology, but now there are steps that can be taken to build security right into the design of these products and systems, and I would expect to see a lot more energy on that part from companies."

A primary challenge with securing the rapidly expanding world of connected devices is the dispersed nature of these products, which makes it difficult to roll out upgrades, patches and other necessary security measures uniformly after the products have left the warehouse, attorneys noted.

"Manufacturers need to make sure both that the devices are individually resistant to cyberattacks, and that the network doesn't provide a pathway into everyone's computer system," said William Tanenbaum, the co-head of the technology transactions practice at Arent Fox LLP, noting that such an intrusion when it comes to industrial products like pacemakers and automobiles could have disastrous and potentially life-threatening consequences.

While federal and state regulators have shown interest in this area and legislative proposals have been introduced to set rules of the road for this largely unregulated universe, attorneys will be carefully tracking how much progress, if any, will be made on either of those fronts this year.

"Present regulatory models do not fit this new field neatly, but the promise of these new technologies is so important that Congress and agencies must address them very thoughtfully," said Sidley Austin LLP partner Alan Charles Raul said.

A more likely outcome is that pressure by consumers will spur manufacturers to pay more attention to cybersecurity and privacy risks, attorneys say.

"If the reason that they can't watch 'Stranger Things' is because their internet-connected devices are taking up too much bandwidth, consumers are going to start to notice and that is likely to be the impetus for change," Jeffer Mangels Butler & Mitchell LLP partner Robert Braun said.

Litigation may help to fill that void and keep manufacturers in check, though, attorneys say.

Edelson said he expects to see more cases over data collection and notice concerns posed by internet-connected devices, which often have small or nonexistent consumer interfaces that make privacy disclosures tricky. His firm during the past year brought notable putative class actions over the allegedly covert collection of data from users of web-enabled vibrators — a matter that settled for $3.75 million in August — as well as Bose's purportedly secret collection and sharing of information about app users' listening habits.

"With new internet of things products being released all of the time, deepening modern technology’s integration into consumers’ everyday lives in increasingly personal ways, new lawsuits over companies’ secret collection and sharing of consumer data is a certainty," Edelson said.

Global Privacy Law Quilt Will Continue to Add Patches

Perhaps one of the most highly anticipated events of 2018 is the implementation of the European Union's sweeping general data protection regulation in May. The law is set to tighten restrictions on the use and flow of consumer data and empower national privacy regulators to levy fines of up to 4 percent of companies' annual global revenues, while continuing to move the EU away from the patchwork and overall less stringent privacy regime in the U.S.

"Once the GDPR is in force, non-EU countries around the world will begin looking at privacy regimes based on the 1995 Directive [which the GDPR will replace] and think about whether they ought to be updated — either to retain adequacy, or simply to keep up with Europe," said Covington & Burling LLP data privacy and cybersecurity chair Kurt Wimmer. "I believe we will have a very busy year working on the introduction and progress of new privacy and cybersecurity laws in non-EU countries."

This international expansion will likely lead to the related challenge of "how to manage ongoing overall confusion from the increasing multiplicity of laws and regulations, particularly as requirements for vendors across industries will grow," Wiley Rein LLP privacy practice chair Nahra added, and other attorneys agreed that increased attention to cybersecurity and privacy issues by policymakers around the world would create headaches for multinationals.

"There will definitely be more and more compliance challenges for companies that face differing cyber regulations in different parts of the world," Halpert said.

The increased attention is likely a byproduct of companies making more use of personal information for purposes such as data mining and regulators wanting to "make sure it doesn't go too far," Overly added, meaning that the interest isn't going away anytime soon.

One of the most obvious areas of divergence is data breach notification. California enacted the first reporting law in 2003, and since then, 47 other U.S. states have followed with their own slightly different notification standards.

Europe has long been an outlier, but the GDPR brings with it a new requirement for companies to disclose data breaches within 72 hours — most U.S. laws require notification as soon as possible, with the handful of states that do set a specific time period going no lower than 30 days. Canada will also soon add to the chaos, with draft mandatory federal breach notification regulations anticipated to come into force in 2018, Krasnow noted.

And in the U.S., attorneys are expecting states to continue the trend of amending their breach notification laws to add more categories of personal information — including data collected from internet of things devices and geolocation information — that trigger notification, while the federal government continues to struggle with long-running efforts to set a uniform breach reporting standard.

"Companies are seeking to comply with different data breach standards, and the conflicts that arise can make compliance costly and burdensome," said Kaufman Dolowich partner Marc Voses. "Companies are hoping for a standard that is more straightforward, and hopefully uniformity will soon emerge."

Attorneys also expect states to continue to grow the legal patchwork when it comes to other hot-button privacy issues, such as the collection and use of biometric data, how schools and their service providers handle students' information, and what companies need to disclose in their privacy policies.

"I expect to see the state attorneys general play a broader role in driving both enforcement and the

overall privacy and security debate," Nahra added. "This likely will be followed by or connected to more state laws addressing specific identified problems, where the federal government has been unable to do anything."

Cyber Insurance Market Will Be a Growth Area

As cyberattacks continue to grow and evolve and privacy risks become more widespread, the market to insure these products is likely to expand with it, attorneys say.

"It will be interesting to see how the insurance market continues to adjust in relation to the potential for significant incidents and whether we see more exclusions in insurance policies for cyber, particularly for catastrophic attacks where there isn't specifically a large-scale insurance solution yet," said Halpert.

Overly noted that companies will need to make sure they're reading their policies very carefully, with an eye toward exemptions for the types of global data breaches such as last year's WannaCry ransomware, which hit scores of companies around the world.

"Insurance companies are going to realize that a single ransomware attack could have two-thirds of the insurance market making a claim, so they're likely to be far more careful about what they're doing in their policies, and companies need to understand that the coverage they're receiving may be far narrower than they think."

Lisa Neal, co-chair of the cybersecurity and privacy practice group at Rutan & Tucker LLP, added that there is still an "open issue as to whether business email compromise, also known as social engineering fraud, is covered by a company’s computer fraud policy."

Two courts recently reached opposite holdings on this topic, Neal noted. The Southern District of New York held in July that a computer fraud policy did cover a claim arising out of a hacker's use of email to trick Medidata employees into wiring $4.8 million overseas, while a Michigan district court reached the exact opposite conclusion in an August decision that held the exchange of emails where a fraudster posed as a vendor to convince American Tooling Center to send payments did not directly cause the transfer of the funds and therefore could not be covered, and both matters will be important to watch as they move up to the appellate level.

“The appeals will likely take a year or more to resolve,” Neal added. “In the meantime, policyholders should closely scrutinize their existing cyber and commercial crime policies to ensure they have adequate coverage for loss caused by email scams.”

Policyholders should also be cognizant of when there may be coverage for cyber-physical losses, such as bodily injury from the hacking of a medical device or property damage from the breach of networked infrastructure or industrial control systems, said Covington & Burling LLP senior counsel John Buchanan.

"Most cyber policies exclude bodily injury and property damage," he said. "Meanwhile, some insurers argue that recent amendments to standard general liability policies — traditionally purchased to cover bodily injury and property damage — now preclude coverage for cyber-related perils. Some insurers have recently touted new insurance products to fill the gaps. But are they actually available at an affordable price, and do they actually accomplish what they claim to do?"

Blockchain Will Find Stronger Footing

Blockchain technology that powers Bitcoin and other virtual currencies made a big splash in 2017, and attorneys expect the prevalence of and uses for the emerging software program that allows transactions to be linked and moved securely using cryptography to only grow in the coming year.

"There's going to be a lot more talk about blockchain in 2018 and its use in a range of applications that play into the privacy and security domain, including the recording of deeds and property and the passing of real property from one entity to the next," Scott said.

Saikali noted that he'll be interested to watch whether companies will introduce the use of blockchain to protect sensitive information, particularly in the financial and health care sectors, which are likely to be "some of the first to implement it."

While blockchain is generally considered a fairly secure way to transfer data, there is still potential for vulnerabilities in any systems created by humans, Braun noted, and the underlying data being sent through the distributed ledger technology, which present their own security risks, could make an enticing target for hackers, who will likely be focused on the less secure "on ramps" to buy, sell and transfer data through the technology, attorneys noted.

"Cyber currency hacks are increasing, especially due to the nature of these assets that make it easy for cybercriminals to take the information and disappear," Devlin said.

--Editing by Philip Shea and Breda Lund.
