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 2019

By **Allison Grande**

Law360 (January 1, 2019, 12:03 PM EST) -- Cybersecurity and privacy will continue to remain top-of-mind for companies in 2019, with the cyberthreat landscape expected to keep growing, vendor relationships taking on added importance, U.S. states continuing to flex their muscles and international data transfers getting even stickier.

Here, attorneys offer five predictions for what promises to be another big year in the cybersecurity and privacy realm.

Phishing and Nation-State Hacks Will Take Center Stage

The past year was marked by major security breaches at big-name brands such as Marriott, Facebook and Google, and attorneys are expecting more of the same in 2019.

"One always benefits by betting on the idea that the cybersecurity problem is only going to keep getting worse," said Seth Berman, the leader of Nutter McClennen & Fish LLP's privacy and data security group.

While the exact shape that cyberthreats will take in the upcoming year is anyone's guess, the recent breach announced by Marriott in late November — which exposed the email addresses, payment card details, passport numbers and other personal travel details of up to 500 million guests at its Starwood properties — gives some indication of what hackers may be looking to target.

"It seems as though we're past the point where hackers are stealing a vast number of credit cards, and instead are going after vast quantities of sensitive data," Berman said. "As we learn about what happened to Marriott and who was involved, we'll begin to understand whether this was a one-off or the start of a trend and what it is that made Marriott an appealing target."

More clarity is also likely to emerge around the methods that hackers most prefer to use to get into systems, with attorneys predicting that the lucrative businesses of deploying ransomware that holds data systems hostage and orchestrating phishing attacks that trick employees into giving up their credentials or other vital information will continue to be significant threats.

"Companies are saying that gathering more data can help them be more sophisticated and streamlined and better understand their customers," said Liisa Thomas, the leader of Sheppard Mullin Richter & Hampton LLP's privacy and cybersecurity practice. "But on the flip side, the bad actors are also thinking

that the more data that they have, the better they can launch bigger and badder attacks against companies."

As hackers accumulate more data, they're able to learn more about how corporate systems work and send targets more realistic-sounding information requests than ever before, and attorneys see no signs of this trend slowing down.

"Particularly in the health care sector, email phishing schemes are getting increasingly more sophisticated and will likely continue to be a major problem in 2019," said Tucker Ellis LLP counsel William Berglund.

Attorneys also expect nation-states such as Russia, Iran, North Korea and China — the last of which has reportedly been tied to the Marriott hack — to continue to be active.

"It's likely that we're going to see more state-sponsored acts from malicious actors," said BakerHostetler partner Eric Packel. "We're dealing with a much more integrated global economy, but at the same time we're also seeing politically much more nationalism and a lot more state-sponsored actors looking to get into systems for not only political purposes but also for the purposes of stealing technology and trade secrets."

Given the evolving political climate and recent escalations such as the Trump administration in September releasing a new national cybersecurity strategy that loosens the rules for when the government can conduct offensive cybersecurity operations, it's likely that nation-state threats "will become a much broader and extensive global problem in 2019," Packel added.

In response to this growing threat landscape, companies in a wide range of industries, from hospitality to tech to critical infrastructure operators, are likely to invest even more time and effort into preparing workers outside their IT departments for breaches and putting together incident response playbooks, according to attorneys.

"I ask clients if they're ready for the big one — a significant cyberattack that threatens their data and even their ability to operate as a business," said Robert Silvers, a Paul Hastings LLP partner and former assistant secretary for cyber policy at the U.S. Department of Homeland Security. "If you're a GC, it isn't enough to lean on the incident response planning of your company's IT security team. You need to know what your legal and compliance teams should be accounting for in those critical first few days of an incident."

Vendor Security Will Loom Larger

When crafting and reviewing data management and incident response plans in the coming year, companies are likely to begin to pay even more attention to an external but vital factor: the role that third party vendors play in handling and safeguarding the personal information they are entrusted with, according to attorneys.

"The first-level attack is generally the main company who, say, manufacturers widgets, and nefarious hackers want to target that company either to steal data or inside information," said Andy Gandhi, a managing director with Alvarez & Marsal's disputes and investigations practice and data risk expert. "But that company has raised its fences and locked its doors, so rather than break into that company, what hackers are looking for is an easier entry point, maybe a law firm that represents the company that may

not have the same fences but may have information about an M&A transaction or a cloud provider that archives its information."

The threat of hackers looking for the weakest link to gain access to corporate systems "gives companies even more to worry about from the perspective of what's happening to their data when it leaves the organization," Gandhi added.

Besides the growing prevalence of third-party hacks, regulatory requirements are also increasingly forcing companies to think more about third-party vendor security, according to attorneys.

Banks, insurance companies, and other financial services institutions and licensees regulated by New York's Department of Financial Services are facing a March 2019 deadline to fully implement landmark cybersecurity rules put in place by the department two years ago.

The rules force covered entities to fortify their cybersecurity protocols by putting detailed data security programs in place, increasing their monitoring of third-party vendors, appointing chief information security officers and reporting breaches within 72 hours. While the regulation has been in effect since March 2017, and there have been several rounds of implementation deadlines already, the final deadline this coming year marks the last chance for companies to comply with the requirement to evaluate the risk that any third party service providers pose to the security of their systems and data and ensure that those elements are protected.

"As a result of those requirements to focus on vendor relationships and the risks that third party service providers present from a security standpoint, vendor management will continue to be an area of very careful focus by a lot of companies in financial services and otherwise," said Locke Lord LLP partner Ted Augustinos, adding that state insurance regulators are also expected to adopt a similar model cybersecurity law finalized by the National Association of Insurance Commissioners this past year.

Federal health care regulators are also likely to pay increased attention in the upcoming year to the risk that vendors and business associates pose to the sensitive patient information they hold, according to Berglund.

"Government regulators are going to increasingly be looking at vendors as being a significant source of risk and look to see what covered entities that have data and share it with vendors do to audit and vet vendors, and we may also start to see more enforcement in that area," Berglund said, noting that the U.S. Department of Health and Human Services' Office of Civil Rights is planning another round of audits assessing covered entities' compliance with the Health Insurance Portability and Accountability Act in 2019.

Additionally, federal agencies are likely to place greater emphasis on third party vendor security when it comes to government contractors in the upcoming year, Crowell & Moring LLP partner Evan Wolff said.

The U.S. Department of Defense in 2016 finalized a contractual clause that requires all of its contractors to have not only adequate security on their own networks and systems that hold defense information but also to ensure that its subcontractors do the same, and the broader Federal Acquisition Regulations are expected to be amended in the upcoming year to include similar requirements, according to Wolff.

"These rules will reach beyond the DOD contracting community to the broader government contracting community," Wolff said.

States Will Continue to Be 'Labs of Democracy'

In a Dec. 13 letter urging Congress to refrain from enacting federal comprehensive privacy legislation that displaces more stringent state protections, a coalition of privacy groups argued that states "are the 'laboratories of democracy'" and have long led the way in the development of innovative privacy legislation, and attorneys don't expect that to change in 2019.

"Until there is some federal privacy statute or norm, we're going to continue to see states be active on these issues and leap-frogging over each other, with each law likely to get more proscriptive as they go along," said McDermott Will & Emery LLP partner Mark E. Schreiber.

State attorneys general are also going to continue to loom large, according to attorneys.

"With every breach and every new privacy law, people are becoming more attuned to what companies are doing with their data," said Alexander Bilus, the vice chair of Saul Ewing Arnstein & Lehr LLP's cybersecurity and privacy practice. "So state attorneys general are going to be very interested in looking at that, and I wouldn't be surprised if we saw more enforcement actions."

While some experts say that they have been somewhat surprised that state attorneys general haven't done more on privacy and security enforcement generally, the past year did include several notable actions by these regulators, including a large group of attorneys general **banding together to hit** Medical Informatics Engineering Inc. with the first ever multistate data breach suit based on alleged violations of HIPAA, and all 50 states reaching a $148 million settlement with Uber over a massive 2016 data breach that the company has admitted it paid the hackers to cover up.

"I will be watching carefully whether these are one-offs or [if] there is a more concerted effort by state AGs on these issues," said Wiley Rein LLP privacy and cybersecurity practice chair Kirk Nahra said.

However, experts agree that state attorneys general won't be silent, and that between them and state legislatures looking to build on recent developments such as California's enactment of a landmark consumer privacy law and Ohio's passage of a data breach litigation safe harbor, states will continue to make noise in 2019.

"We're certainly likely to see more regulation throughout the country, whether it's another law that looks like the California Consumer Privacy Act or more regulation around what's collected and how much data is being collected," Thomas said.

International Data Transfer Landscape Will Grow More Complicated

As data continues to flow around the world, and the global patchwork of data protection and privacy laws continues to expand, companies will likely find themselves spending increasingly more time thinking about the legal risks and roadblocks that may come with transferring and fielding requests to access data internationally, according to attorneys.

Several developments during the past year have further muddied this landscape, including U.S. lawmakers' passage of the CLOUD Act to clarify that warrants for data held by service providers like Microsoft and Google reach data stored anywhere in the world, the European Court of Justice's decision to hear challenges to a pair of popular international data transfer mechanisms and the

U.K.'s vote to leave the European Union.

With the enactment of the CLOUD Act, companies received the legal clarity they were hoping for when it comes to their obligations when law enforcement comes knocking for data stored abroad, but it also opened up new avenues of uncertainty surrounding how other countries will react and what form the bilateral data-sharing agreements that law permits will take.

"It will take some time for many different countries to decide what they want for those executive agreements," said Mark Krotoski, co-head of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice, who added that it also remains to be seen whether other countries will embrace similar standards or move more toward data localization.

A pair of vital data transfer mechanisms — the relatively new Privacy Shield and more established standard contractual clauses — are also currently in a state of flux, with the European Court of Justice set to rule on whether the pair sufficiently protect EU users from U.S. surveillance.

"If the European court rules against those contracts then they could well be invalid from the minute that that judgment is given and companies will have to change immediately, and that would be likely to cause a lot of pain," said McDermott partner Ashley Winton, who is based in London.

Morrison & Foerster LLP privacy and data security group global co-chair Alex van der Wolk, who works in Brussels and London, noted that the European Commission has said that it plans to update the standard contractual clause template in light of the enactment of the bloc's General Data Protection Regulation, although there has been no timetable on when that may occur.

"Hopefully the European Commission will come out before the court case is decided because at the very least that might help to preempt some of the discussion taking place before the court," van der Wolk said.

Data exchanges are also likely to look different coming out of the U.K. in the upcoming year, with the country set to exit the EU in March. Hopes are still high that the U.K. will reach a deal with the remaining bloc members to allow them to continue to transfer data smoothly between the regions, but the possibility exists that there could be a "hard Brexit" that would leave the U.K. needing to meet the same data transfer requirements as countries such as the U.S. that aren't recognized as having adequate data security standards.

"In the case of a hard Brexit, that would pose a problem for companies because they would have to do a lot to make sure that they can exchange personal information with those in the EU," said van der Wolk.

Internet of Things, Cryptocurrencies Will Garner Even More Regulatory Interest

The growing world of home appliances, medical devices, automobiles and other consumer products linked up to the so-called internet of things has been garnering more interest in recent years, and attorneys say 2019 may be the year that more formal regulations or even laws form around these technologies.

"So far there hasn't been a lot of legislation or regulation in this area, but it's becoming a bigger issue, particularly in the health care industry, because these devices are seen as potential entry points for a more systemwide attack on a network," said Berglund. "So we may start to see the federal government

and Congress as well as states possibly look at bills and enforcement actions to regulate this space."

California in September became the first state to enact what attorneys called "modest" rules for security features for internet-connected devices, and there have been several proposals floated by federal lawmakers in recent years to study the industry and create a voluntary program to allow businesses to certify that their internet of things products meet certain data security standards. Additionally, both the Federal Trade Commission and U.S. Food and Drug Administration have issued guidance and recommendations on internet of things privacy and security, and experts don't anticipate this interest waning in the new year.

"Clearly legislators and regulators need to be thinking very closely about areas such as the internet of things, automated vehicles and artificial intelligence, because we're at the dawn of a new information and technology era," said Alan Charles Raul, the leader of the privacy and cybersecurity practice at Sidley Austin LLP. "But if they act proscriptively or overbroadly, they could risk denying society the benefits that these technologies would bring. The hope is policymakers will have the wisdom to restrain themselves from jumping into regulation before they really understand these technologies and their benefits, risks and other implications."

Attorneys also expect more attention to be paid to the growing industry surrounding the sale of digital assets in the coming year.

The U.S. Securities and Exchange Commission in December confirmed that it would continue to keep a close eye on investment firms dealing in cryptocurrencies as the fight continues over whether these assets can be considered securities. SEC Chairman Jay Clayton has been among the high-profile voices that have argued that digital tokens are ripe for oversight and enforcement, while a pair of bipartisan House lawmakers recently floated a bill that would exclude such cryptocurrencies from the statutory definition of a security and thus exempt them from securities laws.

“The SEC has been very active in this space recently,” Berman said. “In 2019, we’re likely to see significant developments and more clear law being developed around these issues, including how initial coin offerings ought to be dealt with and what constitutes a security.”

--Editing by Pamela Wilkinson and Alanna Weissman.