

The Legal Threat Giving Compliance Officers Nightmares

By **Michele Gorman**

Law360 (January 23, 2019, 5:43 PM EST) -- A common worry repeated by compliance officers across industries is about the mass of data their companies collect and how to keep it secure, as businesses of all sizes continue to navigate complex regulatory landscapes and unprecedented challenges from cyberattacks.

While technology affects every organization to varying degrees, compliance officers cite the pressure of the increasingly relevant adage that it's not if but when their organizations will be victims of a cyberthreat.

"A single event can take a highly valuable company and make them worthless overnight — whether that's a data breach, the theft of client money or access to client accounts," said Mathew Keshav Lewis, senior vice president and global head of the regulatory practice at alternative legal services provider Axiom.

Marriott International Inc., for example, has been hit with at least a dozen **putative class actions** in U.S. federal and Canadian courts by customers who said their privacy was violated by a massive data breach in late November that affected **hundreds of millions of guests** and by a shareholder who alleged the company falsely inflated its cybersecurity bona fides.

Here, Law360 looks at the main data security issues troubling corporate compliance officers.

Defending Your Data

More than ever before, companies are collecting and retaining large amounts of data for longer periods of time. Background screening company Checkr Inc., like other businesses, holds a vast amount of personally identifiable information as a result of the more than 1 million checks it runs each month for its 10,000-plus customers.

Given the high volume of data the company collects, privacy and security data features are one of the biggest concerns for Irene Liu, Checkr's general counsel responsible for leading its legal, compliance and government relations teams.

"Data is incredibly important, incredibly valuable," she said. "But at the same time, it's something that keeps us up at night."

Liu said she had similar concerns in her previous roles at the U.S. Department of Justice, Federal Trade Commission and tech companies BlackBerry Ltd. and Lookout. But the risks — and therefore, the worries — are magnified now, as data is more readily accessible. And the threat of a large data hack sometimes falls on legal, which concerns her.

Liu's fear is valid. Some top lawyers have been personally affected by high-profile security incidents. In March 2017, Ronald Bell **resigned** from his general counsel post at Yahoo Inc. in the wake of an internal probe that found certain senior leaders failed to adequately respond to a trio of data breaches believed to have affected at least 1.5 billion users.

Since their functions are often tasked with identifying and mitigating risk, in-house counsel and

Since their functions are often tasked with identifying and mitigating risk, in-house counsel and compliance officers play a key role in helping their businesses prepare for possible data breaches. When a cyberattack occurs, the possible activities that fall on the legal team include properly handling a forensic investigation, coordinating with law enforcement, dealing with concerned regulators and communicating details to key business stakeholders and the public.

Liu and other corporate lawyers say they find comfort in proactively spearheading an incident response plan that identifies the individuals who comprise the receptive team, as well as their contact information. Sometimes they perform simulated breaches that bring together the key members who would be involved in the response — the general counsel, CEO, chief financial officer, chief marketing officer, chief operating officer, head of information technology security — to work through a mock incident in real time.

Liu said she can also sleep better knowing the company has completed or is working toward solutions to mitigate risk, such as having superior cyber insurance. And developing relationships with Checkr's security and technology teams helps her remain aware of any cybersecurity gaps at the company.

Operating in a New Regulatory Era

The European Union's General Data Protection Regulation enacted in May forces companies or firms in any country that offer products or services to EU residents or that store and collect data on those individuals to gain explicit consent to keep personal data and allow consumers to have their details deleted.

The GDPR applies to the large majority of organizations, whether they are in the U.S. or the EU. Under the new regulation, companies could face stiff fines if they break the rules. France's privacy authority, for example, **on Monday** hit Google LLC with a nearly \$57 million fine for allegedly failing to clearly explain how consumers' personal information is being used.

Since the GDPR's enactment, states like California have passed their own similar privacy laws, which are expected to present challenges for companies operating in many of these jurisdictions.

"It is concerning because now you have all these nitty-gritty, different laws to comply with, and that makes it harder," Liu said.

William Welch, deputy general counsel, litigation and chief compliance and ethics officer at Voya Financial Inc., said the California law is at the top of his list of compliance concerns. Even though the directives of the bill aren't expected to take effect until 2020, the planning to construct the needed infrastructure for compliance takes time to implement.

The GDPR and landmark privacy bill in California, which will give consumers the ability to control how online companies use and share their personal information, indicate to businesses around the world that they not only need to have the proper tools in place to fight cybersecurity threats, but they must meet their commitment to clients, said Lewis from Axiom.

Under these new regulations, companies must understand the data they keep, which includes knowing whether data is on internal servers or outsourced to third-party vendors. Being more aware of the types of data can help a company more quickly determine the information that might be at issue from an attack, as well as the scope of a possible breach.

Preventing Third-Party Risk

The growing interconnectedness of the world is forcing companies to have a greater understanding of their supply chains and the commitments they've made to clients, experts say. Within this framework, they advise in-house counsel to fully vet a third-party service provider to make sure they've set up proper security protocols and comply with the statutes and regulations that govern them. Companies should also ensure they establish proper contractual provisions with vendors, experts say.

Several previous and well-known cyberattacks have in some way involved subcontractors. In the 2013 Target Corp. breach, for example, cyberattackers **accessed** the retailer's server through

stolen credentials. The breach affected more than 41 million customer payment card accounts and contact information for more than 60 million customers.

A year later, hackers used vendor login credentials **to break into** The Home Depot Inc.'s payment systems, and millions of customers' payment card information was exposed.

Welch said he worries about the robustness of third-party vendors that collaborate with Voya.

"That's just one more avenue that some external party with malicious intent can potentially do something with respect to Voya," he said.

One way he has managed to lessen this fear is by governing the company's relationships with subcontractors.

"You'll be amazed at how much more you get in terms of information when you're having a face-to-face [meeting] or a conference call," he said.

He also mentioned how it helps to adopt vendor codes of conduct, scrutinize media reports for unfavorable news about vendors — and confront them, if necessary — and require vendors to explain their cybersecurity programs with documentation to corroborate their claims.

Because of the vetting process, Shon Ramey, general counsel with software and services company NAVEX Global who oversees the global privacy function, said he finds at least some comfort in knowing the company controlled what it could.

"That's the only way you can get a little more sleep at night," he said.

Watching Out for Inside Threats

Some industries are undergoing evolutions in sizing, direction and strategy, which can cause internal dysfunction and adversely impact individual employees. Within their own companies, some in-house counsel and compliance officers said they worry about disgruntled employees who might download or send information that could be harmful to their companies.

Other in-house attorneys said they're concerned about the unknown threats and developments that could impact their organizations in the future.

"It's a big world with a lot going on, and there's a fair amount of wanting to ensure that you are doing everything well that you possibly can," said Eric Tuchmann, senior vice president, general counsel and corporate secretary of the American Arbitration Association. "Everybody thinks about [the unknown] and they try to anticipate and you do your best."

And with social media and other technological advancements altering people's habits, employees have the ability to establish a platform to express their views. But some lawyers fear the message could involve proprietary or confidential information that could have harmful consequences for companies.

"Times have changed," Welch said. "With that changing of the times, this threat has increased dramatically as well."

--Additional reporting by McCord Pagan, Joyce Hanson, Allison Grande, Steven Trader and Emily Field. Editing by Katherine Rautenberg.