Five areas in which Marriott data breach raises red flags for financial firms

Published 06-Dec-2018 by
Richard Satran, Regulatory Intelligence

Financial services firms are often ranked as the best prepared of all sectors in protecting client data and putting cyber controls in place. But the massive data breach at Marriott International this month pointed to rising risks in every sector and five key areas where financial firms may need to make significant upgrades in safeguarding data.

The incident in which intruders gained access to a half-billion customer accounts at the world's largest hotelier has been declared the second largest such case on record, topped only by Yahoo's breach exposing personal data from 3 billion personal email accounts. Marriott International faces fines and lawsuits that could be the largest ever since the Europe's General Data Protection Regulation imposes fines well into the billions of dollars.

Financial firms have data concerns

Financial firms have been seen as less vulnerable than other industries because of their long history of managing clients' money on secure global networks. The highly regulated environment in which they operate has also made them safer bets.

But the rapid expansion of banks and brokers into online retailing poses new challenges not unlike those faced by global firms like Marriott, not least being a major push by regulators in many jurisdictions to put GDPR-like privacy protections in place.

Other countries are looking at upgrading their rules to harmonize but have been taking differing approaches suited to their jurisdictions and privacy standards. The unifying theme in nearly every jurisdiction has been that personal data has immense value and fines should be just as large.

Key areas of risk for banks in being digital

Banks are not the main target of the European Union's GDPR, whose key concern has been the wholesale monetization of personal data by social media and internet business aggregators. But its rules apply to finance firms that hold large amounts of personal data, as did Marriott's loyalty program. The Marriott breach remains under investigation by the company and regulators. But already it flashes warnings for financial firms. Here are five key concerns:

• 1-**The Marriott breach showed the security challenge of building online retail operations that banks could also face in their own expansion of online customer services.** In one recent example, the Financial Industry Regulatory Authority last month fined the large investment firm LPL Financial $2.5 million over alleged inadequate protection against cyber intrusions. The risk report issued by the U.S. Office of the Comptroller of the Currency put cyber attacks at the top of its list. "These threats target large quantities of personally identifiable information and proprietary intellectual property and facilitate misappropriation of funds at the retail and wholesale level," the OCC said.

• 2-**The breach underscores the need for financial firms to have regular cyber security risk audits.** A foundational part of most cyber defense programs, such audits were a key element of GDPR as well as the groundbreaking New York State Department of Financial Services cyber regulations that took effect two years ago. The use of penetration testing was also underscored. "Marriott should have had a well-resourced cybersecurity team in place to constantly probe their networks and systems for weaknesses, ideally scaled via incentivized ethical hackers. Had this been the case, such an extended breach simply could not have happened," said Simon Migliano, head of research at Top10VPN.com, a cybersecurity research consultant.

• 3-**The problem for Marriott arose in its Starwood Hotels & Resorts unit acquired in 2016; this showed the risk of data protection in mergers and acquisitions, in which finance firms have broad exposure.** Investment bankers face due diligence responsibilities in which assessing cyber-risk is a key factor. More importantly, large banks and brokers are challenged with continually integrating sensitive data in acquired units as well as branch offices, foreign affiliates, counter-party ventures and third party vendors. The OCC saw elevated risk when firms do not "fully integrate appropriate management information systems, operational platforms, internal controls, and risk management after mergers or acquisitions."

• 4-**The breach showed that financial firms need to prepare for cyber threats that OCC said were becoming "more sophisticated and more global."** Marriott reported that the intruders appeared to have penetrated the company's network deeply enough to use its encryption tools to avoid detection over a period of years. Cyber attackers frequently cover their tracks by creating layers of network code that disguises the source of intrusions. The Securities and Exchange Commission has called for more funding to meet complex cyber risks and to remain relevant as fintech takes over the securities industry. The OCC has warned bankers that online attacks are "increasing in speed and sophistication."

• 5-**The new attack shows that compliance teams must have an enterprise-wide overview of vulnerabilities in personal data used by the firm.** Compliance must play a key role in mitigating regulatory and reputational risk, especially in spotting and reporting events quickly. Many regulators are now requiring notification within 72 hours. The demands of GDPR and cyber protection require chief compliance officers to have "visibility into the data flows throughout the whole enterprise," said Matt Kelly, chief executive officer of Radical Compliance, in a NAVEX Global blog.

The OCC has cited the need for “enterprise-wide” programs so firms can spot signs of intrusions and suspicious activities wherever they arise. In one recent case Capitol One, one of the largest U.S. financial services firms, was cited for anti-money laundering control lapses and ordered to pay $100 million to settle a case blamed on a former check-cashing unit. The firm told analysts its OCC consent order required a cross-unit solution involving “better risk management, along the credit dimensions, fraud, cyber security and product deployment."

Regulators are not expecting perfection in curbing attacks but are pushing firms to have protection in place and a plan to mitigate damage and prevent its spread. While GDPR and rules from other regulators have upped the stakes for failing to institute protection of personal data, the EU and other authorities are working with firms on corrective measures to comply with its provisions. They have thus far held off on imposing fines. The NYDFS as well has worked with firms in adopting its rule.

"Breaches are inevitable," Migliano said. "All it takes is a single staff member to click on a phishing email or a hacker to stumble on a new vulnerability. The only effective cyber defense strategy is to accept that reality, get on the front foot and focus on detecting intrusions and vulnerabilities as rapidly as possible and responding in kind to minimize their impact.

(By Richard Satran of Thomson Reuters Regulatory Intelligence.)

Produced by Thomson Reuters Accelus Regulatory Intelligence 13-Dec-2018