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

Banks Face Cybercrime Wave As Tougher Regulations Loom

By **Mark Taylor**

Law360, London (January 24, 2017, 10:54 PM GMT) -- The financial services sector is suffering an unprecedented wave of cyberattacks in both scale and number, and lawyers told Law360 that businesses must radically alter their thinking on defense and response as regulatory pressures mount.

Early next year, the Directive on Security of Network and Information Systems, General Data Protection Regulation, Directive on Payment Services and Open Banking initiative all enter force. The latter pair will force banks to become more open to technology while the former will punish them heavily for any slip-ups at a time when they are more exposed to digital threats than ever.

"We know cyber risk is a daily threat and that cybercrime is here to stay. It will increase in prevalence; it will increase in sophistication. It is a permanent risk that should be firmly on all boardroom agendas," said Simon Shooter, partner at Bird & Bird LLP. "We started the cyber group in 2010, and it's taken seven years of chiding to get the message through that cybercrime presents a real and dangerous risk."

Almost one year ago, $81 million was stolen from the Bangladesh central bank from thieves who gained access to the Society for Worldwide Interbank Financial Telecommunication international transactions network. Later in the year, Tesco Bank in the U.K. was hacked, prompting calls from lawmakers to create a single regulator for cybersecurity as the lender was forced to repay customers millions of dollars. This week, Lloyds Banking Group became the latest big name added to the list of the breached as details of a denial of service attack on the lender two weeks ago emerge.

And these are merely the incidents that make it into the public domain. Starting next year, firms will have a duty to publicly inform, which brings issues of reputational damage into play, as both the GDPR and NIS contain new requirements to report breaches to regulators and notify security incidents that affect the continuity of supplying financial services.

"The GDPR is a massive text with groundbreaking change in the data privacy area, in terms of compliance requirements and the new personal data breach notification rule," said Mark Young, data privacy partner at Covington & Burling LLP.

Lawyers say banks are privately fending off attacks of increasing sophistication every single day as a new

breed of digital attackers probe for the many new points of entry to a system, from mobile and internet banking to exploiting staff.

“The major banks have areas of extremely competent and market leading cyber resilience, but a challenge to their cyber resilience can often be raised by the nature of banking with siloed behaviors,” Shooter said.

The lack of a uniform approach in banking where splits occur across various business lines can lead to vulnerability, Shooter added. While they may operate well independently, the many different departments of a bank, sitting across various continents in the case of the big names, often do not work well as a whole when it comes to cybersecurity, lawyers said.

Banks also have hundreds of thousands of employees, including contractors, who have different privileges, according to Craig Rogers, partner at Eversheds LLP.

“There is a complex supply chain, so how do you actively check and monitor all of those people and make sure they don't expose you to vulnerability?” he asked.

Many financial services firms have been quick to realize that their weakest point, where many cybercrooks are able to gain entry, is via staff, according to Rogers.

“Methods of attack shift on a daily basis. It’s a bit like fighting diseases; they morph and develop, and the security responses follow shortly after,” said Shooter. “It is a game of catch-up, so when developing a defense playbook, the aim is having the best stab but also to acknowledge that the playbook will need to adjust to the relevant circumstances.”

As a result, compliance costs in relation to cyberdefenses are soaring, and Britain’s biggest banks are leading the charge to fight back.

Last week, HSBC Holdings PLC announced the formation of a technology advisory board of senior CEOs from around the globe to help the bank take advantage of technological innovation, combat cybercrime and leverage its global infrastructure. It echoed a similar move by Banco Santander SA last year.

“You have innovation groups looking at customers, but there is a separate group looking at regulations and compliance, and it’s all about marrying them up,” Rogers said. “A lot of what they are trying to understand is where the next trends are in the development of mobile banking, for example, such as moving to a more distributed model, and how safe that is.”

A significant new initiative on this and other such groups’ radar is Open Banking, which comes into force in January 2018 and is aligned with the PSD. It will require Britain’s banks to open their systems to new technology companies offering consumers a wider array of digital banking products, all in the name of competition. For banks, this has been a major security concern and fierce point of lobbying.

“PSD and Open Banking are also really shaking things up. There is a lot of thinking in how they will change security around that,” Rogers said. “In Open Banking, you are providing a gateway to your infrastructure, so banks think about how consumers are locked in and not exposed them to security risks."

Other financial giants are taking what regulators call a “holistic approach” where their aim is to bring together the variant parts of the business and ensure everyone is clued in to the dangers.

For example, Barclays PLC has recently opened a multimillion-dollar Joint Operations Center in London's Canary Wharf, aligning information technology with information security and cybersecurity teams on a secure floor in what appears to be a first for banking and rarely seen outside of military or law enforcement. The bank declined to give more detail on the center, but a person familiar with the matter said the British giant has drafted in government intelligence experts to oversee operations.

“As a global bank, Barclays is at the crosshairs of cybercriminals,” it said in a statement. “As an organization that processes financial transactions, stores and transmits sensitive client information and participates in the global financial marketplace, Barclays is an attractive target to organized criminals, hackers and hacktivists.”

The bank said it is expecting “a continued increase in the number and sophistication of cyberattacks against it, its partners and its employees and clients.”

The reason banks are forming security teams and building defense centers is that the sector has become defined in the same way as power grids, said Jennifer Martin, of counsel in the Silicon Valley office of Covington & Burling LLP.

“If you want to disrupt the financial industry and economy, attack the actual networks, the computer systems," she said. "There is a lot more focus from regulators, certainly in the U.S., as well as in the G-7 Nations, on threats to the financial services industry as a critical infrastructure."

Barclays and other big names are tooling up ahead of the incoming regulations. While Lloyds has done all it can to keep details of the attack it suffered out of the public domain, it will no longer have that privilege under the GDPR, as it will be forced into mandatory disclosure as similar U.S. breach laws.

There is also a demand on the industry to seek more clarity from regulators.

“The new laws, GDPR, PSD, NIS all come into force around the same time next year, and as usual, a lot of the regulators in this area don’t cooperate when it comes to guidance,” said Toni Vitale, legal director in the data and information team at Addleshaw Goddard LLP.

He said one example of regulatory arbitrage can be found in how the Britain’s finance sector watchdog and its data protection chief take different positions on issues such as messages to clients.

“The Financial Conduct Authority and the Information Commissioner Office take a differing view on what is marketing and what is a service message,” Vitale said. “It’s a very difficult area to navigate because if the regulators can’t get their act together, there is little hope even for the big banks, who have huge compliance teams, internal and external legal teams and everything else, to interpret the overlap between the various regulations and how they work together.”

He added that it is becoming increasingly difficult to navigate a path through the regulatory maze despite spending a lot of money on compliance and the sector pumping tens of millions more each year into this.

“It will be a big year in terms of compliance but also how the banks will position themselves to ensure they maintain their reputations,” Vitali said.

Lawyers agree that training and practice drills are crucial, and banks should be well-versed in how to respond should the unthinkable occur. The alternative, as Shooter pointed out, is fines, which have a less predictable future as the British government has not yet confirmed how draconian the penalties will be.

“The GDPR has the glitzy sanctions headline of 4 percent of aggregated annual global turnover for fines,” Shooter said, adding that national regulators will set the sanction breach for NIS legislation, which could become problematic when taken together. “If you get fined 4 percent for the success of the attack on the network and systems and 4 percent of the loss of data, most businesses would be on their knees as a result of the aggregated fine."

Britain’s finance conduct watchdog is also looking at the potential for punishing firms that have poor incident response plans.

“The FCA has data security as a main priority going forward. It’s clear in their business plan and recent messages to the sector,” said Ian Hargreaves, fraud investigations expert and partner at Covington. "They are increasingly concerned about attacks; they are aware of the potential impact of such threats not only in relation to market integrity but to the nation state itself.”

He added that it has taken a while for the regulator to finds its feet in the data protection world, but it is catching up quickly and pushing its message of zero-tolerance for failures.

“The FCA is now getting the message out more forcefully; the fines are likely to increase,” Hargreaves said. “It’s a significant development, some would say overdue, but they are addressing the issues as are many financial institutions.”

--Editing by Christine Chun and Kelly Duncan.