Author
Jason Elmer
Managing Director
Compliance and Regulatory Consulting
Duff & Phelps
jason.elmer@duffphelps.com

Preparing for and Responding Effectively to Cyber Attacks

Cybersecurity is the biggest risk facing the financial system, according to outgoing SEC Chair Mary Jo White, and as such firms can expect it to increasingly be a regulatory focus going forward. As she put it, "We can't do enough in this sector."[1]

It's not just the rhetoric that has reached new heights; in June, the SEC appointed IT security expert Christopher Hetner as a senior adviser "coordinating efforts across the agency to address cybersecurity policy."[2] In addition, cybersecurity compliance was among its examination priorities in 2016 and is likely to carry on into 2017.

So far, the SEC hasn't mandated specific standards for firms. Nevertheless, the agency has already taken enforcement action in cases where it has deemed that inadequate cybersecurity policies and procedures fall foul of the federal "Safeguard Rule" – Rule 30(a) of Regulation S-P under the Securities Act of 1933.

"Firms must adopt written policies to protect their clients' private information, and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs," it noted.[3]

A worldwide focus

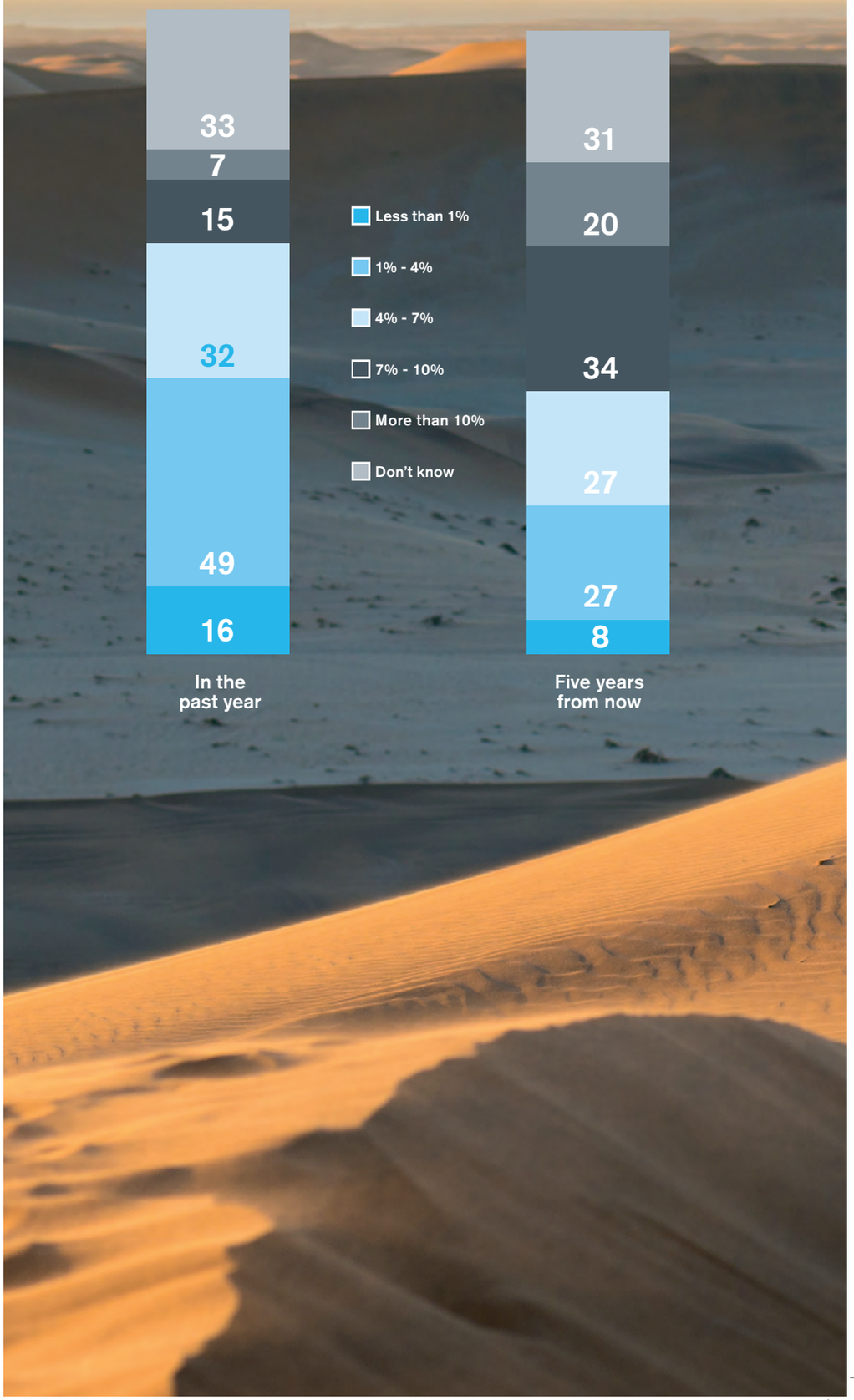
The SEC is far from alone among U.S. regulators in focusing on cyber issues. In March, the National Futures Association's (NFA) Cybersecurity Interpretive Notice, approved by the Commodity Futures Trading Commission, came into effect. Regulated businesses must have an information systems security program appropriate to their circumstances, even if there is flexibility in determining what that is. In May, FINRA too published a checklist for small firms creating a cybersecurity program.[4]

Financial regulators elsewhere are also increasingly taking the mantle from – or perhaps more often working with[5] – the data protection bodies that have driven enforcement of cybersecurity standards to date.

Laying out the UK regulator's approach in September, the FCA's director of specialist supervision said it intends to broaden its existing focus on the largest financial services providers to include smaller firms.[6] In a circular in October, Hong Kong's FSC, meanwhile, identified cybersecurity management as a priority for its supervision, noting the number of hacking incidents it had seen in the past year.

1 http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4
2 https://www.sec.gov/news/pressrelease/2016-103.html
3 https://www.sec.gov/news/pressrelease/2015-202.html
4 http://www.finra.org/industry/small-firm-cybersecurity-checklist
5 https://www.fca.org.uk/publication/mou/mou-fca-ico.pdf
6 https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms

AS A PERCENTAGE OF ANNUAL REVENUE, HOW MUCH DO YOU BELIEVE YOUR COMPANY SPENT OR WILL SPEND ON COMPLIANCE?



"While these hacking incidents are still under police investigation, there are indications that brokers and their clients may be able to do more to better protect online trading accounts," it said.

Whether this interest from regulators will bring about new rules remains to be seen, but increasing attention – and enforcement action – under existing requirements seems likely. Even without this, though, it is worth noting that increasing and high-profile attacks are prompting investors to ask many of the same questions about cybersecurity as regulators are posing. Commercial forces, as well as regulatory pressures, are ultimately likely to prove key in improving standards.