Cybersecurity

Cybersecurity is the biggest technology anxiety among those regulating financial advisors this year. So what counts as a cyberattack? and what do analysts suggest that smaller companies do?

Cybersecurity is the biggest technology anxiety among those regulating financial advisors this year. That's partly related to a 2016 hack of the Securities Exchange Commission's ("SEC") EDGAR system of online public filings, and also because of the SEC's new cybersecurity unit set up in response to that breach. Cybersecurity has been a top issue for the financial services industry for years now, and with good reason: companies in the financial services industry face tens of thousands of cyberattacks each day. So what counts as a cyberattack? IBM's recent study of cyberattacks in the financial services industry defines attack as one "that is attempting to collect, disrupt, deny, degrade or destroy information system resources of the information itself." In shorter terms, cyberattacks now include more than just hacking, they also include hijacking.

"Cybersecurity is the biggest technology anxiety among those regulating financial advisors this year. So what counts as a cyberattack? and what do analysts suggest that smaller companies do?"

Cyberattacks involving hacking of banks usually target smaller or non-domestic banks, such as the 2016 hack that transferred $81 million from the bank of Bangladesh. Cyberattacks involving hijacking, like wannacry, the ransomware attack that crippled healthcare companies also disproportionately impact smaller or international companies. For example, in June of 2017, ransomware attacked the property wing of BNP Paribas, France's largest bank. Just as with the wannacry virus, the issue involved in the BNP Paribas attack may have involved older technology that was not updated.

In 2014, the SEC adopted the Regulation Systems Compliance and Integrity ("RegSCI") to "strengthen the technology infrastructure of the U.S. securities markets." That new regulation applied to stock exchanges, FINRA and other self-regulatory organizations. The SEC also intended, through RegSCI to increase its regulation, through oversight and enforcement, of market technology infrastructure. Hacks into the market exchange are rare and, more importantly, rarely cause problems since an irregularity in an exchange is corrected by temporarily shutting it down.

Importantly, while exchanges are reported on internet sites and can be monitored that way, the actual systems themselves are not connected to the internet. The exchanges themselves have circuit breakers, a limit to the amount of change that can occur, before an automatic stop to trading will occur. For the New York Stock Exchange, those points are 7%, 13% and 20% of total loss in one day.

While RegSCI aimed its regulation updates at the marketplace, new regulations from the SEC may aim at the market players, including those small firms at risk of cyberattack. The new threat is not to the marketplace, but to businesses. According to one study, 43% of all cyberattacks targeted small businesses. Other reports found the financial services industry is hacked more often than any other resulting in more than 200 million records being breached in 2016, an exponential increase each year. New regulations to be put into effect in May of 2018 in the European Union also reflect this trend.

As discussed in other articles, available on our blog at: https://www.bcgbenefits.com/blog/erisa-and-enterprise-clouds the Department of Labor has issued advisories about keeping client and individual investor's information secure, including reducing risk through: 1) data management; (2) technology management; (3) service provider management; and (4) human capital management (background checks and training). It stands to reason that the threat that the SEC regulators seek to manage in the near-term might fit into the second

continued ...

Cybersecurity

Cybersecurity is the biggest technology anxiety among those regulating financial advisors this year. So what counts as a cyberattack? and what do analysts suggest that smaller companies do?

category, of technology management. While its unclear whether that oversight will include enforcement actions, such as to penalize firms for failing to prevent possible hacks, increased scrutiny in compliance is possible.

Many analysts say that the key to new cyber security is the ability of a company to adapt and respond. New technologies that enhance those qualities often focus on early detection of unusual patterns.

In the financial services industry, clients and customers act in predictable ways. Layers of passwords and encryption enhance a customer's feeling of security, making it easier to prevent cyberattacks on client information to some degree. And, that predictable behavior can all be stored in a database to be analyzed for outlier activity. Endpoint Detection and Response technology focuses on that behavior and database catalog to prevent malware like ransomware from getting a foothold into a networked system. Ransomware (like wannacry) may be able to access systems, but it won't necessarily act in the same patterns as users typically do. Thus, IS departments could be alerted through EDR systems to a possible intrusion.

Similar to EDR, **User and Entity Behavioral Analytics** ("UEBA") technologies also focus threats originating inside the system by examining user behavior but include not only endpoints but networks and applications as well. Both EDR and UEBA focus on the analysis of the information to indicate a variant in the norm, rather than sounding an alarm about a specific event. By analyzing the data from system logs, event notices and other tools, they can highlight emerging problems.

Cloud Access Security Brokers ("CASB") also may be a vital technology to deploy in preventing cyberattacks. CASB is a tool (or service) that interacts at the intersection of a company's onsite infrastructure and their enterprise cloud provider's infrastructure. By doing so, the CASB allows a company's security policies to reach beyond their own network.

The financial services sector was an early adopter of **data visualization** tools, often used by law enforcement, to detect fraud. Analysts now point to these tools as extremely helpful in preventing cyberattacks. While EDR and UEBA technologies help analyze data patterns to detect potential invaders into a company's information infrastructure, visualization tools allow companies to see patterns. Companies like Keylines https://cambridge-intelligence.com/keylines provide graphs and charts showing data for financial institutions that helps spot patterns in what might appear to be unrelated sets of data flows.

Finally, some analysts suggest that smaller companies look into cyber insurance. This business insurance, different from a general liability policy (which usually does not cover hacking or hijacking), covers the cost of data recovery. Some policies also cover Attorneys' Fees if the cyberattack causes harm to clients whose information was obtained, but those analysts also recommend reading the fine print on policies to make sure Attorneys' Fees are included in the policies. ■