Securities meet cybersecurity: how companies can face mounting threats

By Roger E. Barton, Esq., and Kenneth N. Rashbaum, Esq., Barton LLP

MAY 16, 2022

The Securities and Exchange Commission (SEC) is upping the ante in the fight against cybercrime. In 2022, a host of new proposed rules directed at public companies, registered investment advisors (RIAs), and investment funds are creating a more robust framework by which these entities must report incidents and make investor disclosures related to cybersecurity.

On Feb. 9, the SEC released a rule proposal homing in on cybersecurity risk management among RIAs and investment funds (Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies — SEC.gov). If finalized in their current form, these rules would require these entities to adopt written policies and procedures to bolster defenses against potential cybersecurity attacks. The rules would also mandate the reporting of cyber incidents to the SEC, as well as the disclosure of material cybersecurity risks to clients and investors, including any cyber incidents having occurred within the previous two fiscal years.

While cybersecurity risks cannot be eliminated entirely, they can be considerably reduced, and many of the risk mitigation strategies are decidedly low-tech.

Only a month later, on March 9, the SEC released another rule proposal — this time aimed at public companies' reporting obligations — that would help "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting" (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure — SEC.gov).

This rule proposal is fairly expansive and would require public companies registered under the Securities Exchange Act of 1934 to:

- Report material cybersecurity incidents within four business days of discovery of the incident;
- Provide updates regarding previously reported material incidents;
- Disclose if and when "a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate";
- Detail the company's policies and procedures for identifying and managing cyber risks;
- Expound on the role of the company's board of directors and company management in managing cyber risks, implementing policies, and providing oversight;
- Disclose whether any board members have cybersecurity expertise and, if so, detail the nature of the expertise.

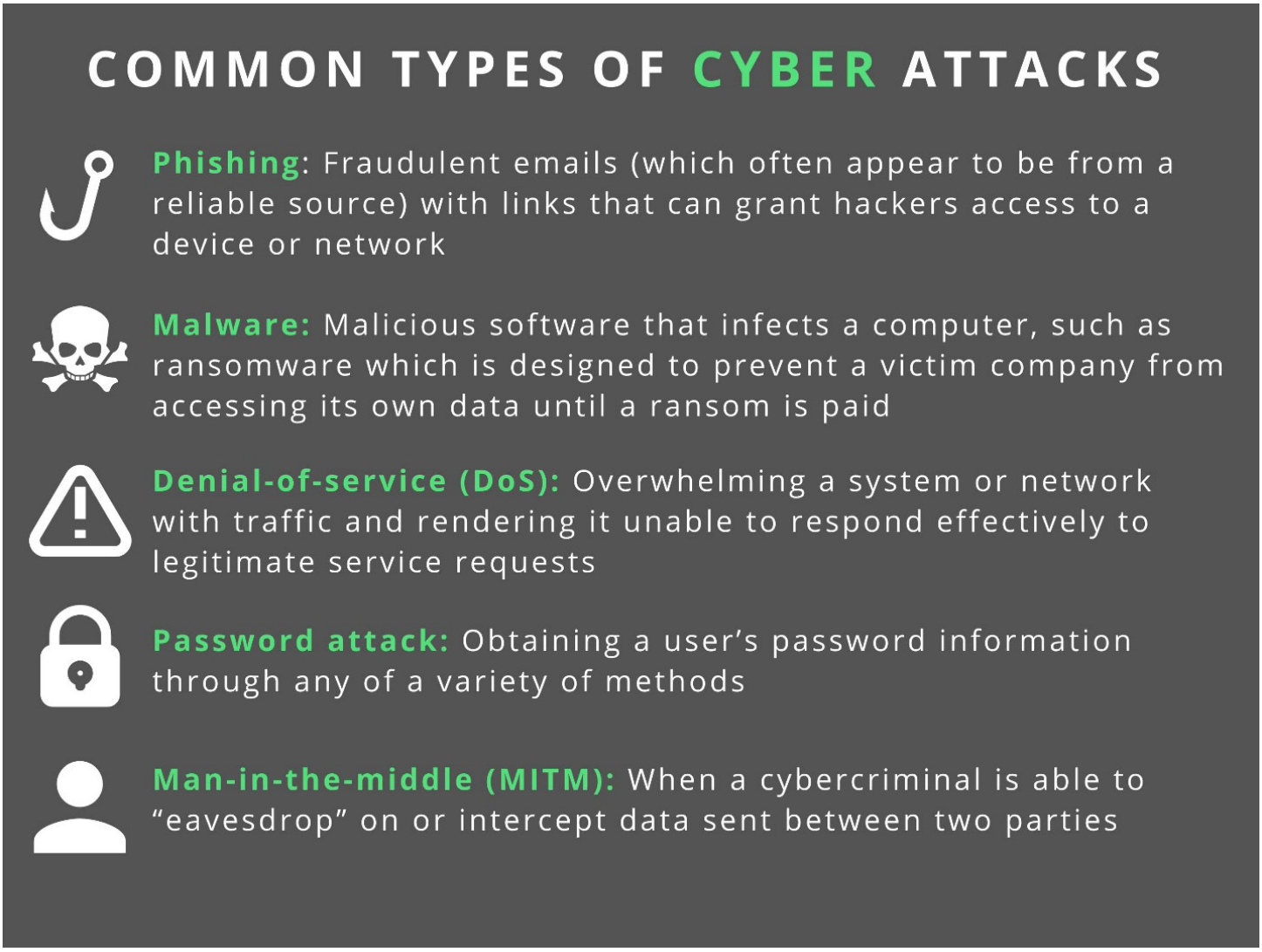
Both of the SEC's rule proposals coincide with a greater national focus on cybersecurity, namely the Cyber Incident Reporting for Critical Infrastructure Act signed by President Joe Biden on March 15. The act will require companies considered integral to U.S. infrastructure (i.e., ones critical to national security, economic stability, and public health/safety) to report significant cyber incidents within 72 hours and any cyber-related ransom payments within 24 hours.

The rising global threat

The recent attention on cybersecurity resilience is certainly not unfounded. According to the Check Point 2022 Security Report, global cyberattacks against corporate networks increased by 50% in 2021 in comparison to 2020.

Part of this deluge of cybercrime can be attributed to the reverberating aftershocks of the COVID-19 pandemic, including the number of advisors and company employees working from home without the security controls offered by office information systems software (e.g., instances where routers had not been rebooted in many months; out-of-date security software; family members sharing devices, etc.) This shift to a greater reliance on remote work has presented new vulnerabilities for hackers to exploit.

Additionally, after the pandemic's onset, many malicious phishing emails took the guise of being related to COVID-19 health or vaccine information to successfully lure in unwitting victims.



Credit: Graphic provided by the authors' firm

One cybercrime tactic that gained steam in 2021 was the deployment of ransomware. In February 2022, the Cybersecurity & Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory with authorities from the U.K. and Australia warning of an uptick in ransomware attacks during 2021 (Alert AA22-040A: 2021 Trends Show Increased Globalized Threat of Ransomware).

While the advisory notes that many of the victimized companies in 2021 were high-value targets (such as the Colonial Pipeline Company, JBS Foods, and Kaseya Limited), the FBI has "observed some ransomware threat actors redirecting ransomware efforts away from 'big-game' and toward mid-sized victims to reduce scrutiny," the advisory states. That is to say, regardless of size or sector, virtually any company has the potential to become a target for malicious actors.

What companies and advisors can do

While cybersecurity risks cannot be eliminated entirely, they can be considerably reduced, and many of the risk mitigation strategies are decidedly low-tech. Some can be implemented without third-party forensic consultants. More significantly, though, they may be required by best practices, clients (particularly institutional clients), and carriers of technology errors and omissions and professional liability insurance.

Review, update, and test the security incident response plan. The time to see if the plan works is not when the red skull appears on your screen.

Implementation and documentation of the following safeguards can reduce legal risk, but also business risk that could arise from loss of the company or advisor's reputation and the confidence of investors following a successful cyberattack.

(1) Prepare a data inventory and map showing what personal and protected financial information you have, where it is used and

stored, how it is backed up, and with whom it's shared. It is difficult to protect information unless you know it exists, where it is located, and how it is used.

(2) Implement Multi-Factor Authentication ("MFA"), in which login requires the entry of a code sent to a smartphone for access to information systems.

(3) Conduct the next scheduled system scan and risk assessment now, including attempts by "white-hat" or "ethical" hackers (i.e., non-malicious hackers that have been hired to probe for security vulnerabilities) to enter the system in the manner of a true attacker, an actual malicious actor looking to steal or disrupt data. These assessments and scans can reveal the presence of malware that may not yet have resulted in a data breach.

(4) Anti-malware or antivirus software should be updated automatically to scan regularly for malware.

(5) Review (with an insurance or legal professional if necessary) your technology errors and omissions, professional liability, and cyber liability insurance coverage to ascertain if it covers the threats in the current cybersecurity landscape, including potential regulatory penalties for violations of the finalized SEC rules.

(6) Review, update, and test the security incident response plan. The time to see if the plan works is not when the red skull appears on your screen. Similarly, review and update the business continuity and disaster recovery plan that would require implementation in the event of a ransomware attack or natural/man-made disaster.

(7) Train the workforce on security awareness and, in particular, alert IT if the employee notices slow or unusual system behavior.

While the above precautions are not a guarantee that a cyberattack will not occur, they can help to mitigate the risk posed by cyber threats, while also garnering the confidence of investors and ensuring compliance with the SEC's new requirements for disclosing cybersecurity policies and procedures. In a business world that is becoming increasingly reliant on technology and digitization, the need for heightened cybersecurity cannot be understated. As mentioned before, the time to enact a plan is not *after* a breach has occurred — it's right now.

Roger E. Barton is a regular contributing columnist on securities regulation and litigation for Reuters Legal News and Westlaw Today.

About the authors

Roger E. Barton (L) is the managing partner of New York City-based **Barton LLP** and a litigator. He represents clients in the capital markets and financial services industries regarding securities fraud, breach of fiduciary duty, common-law fraud, 10b-5 class actions, and breach of representations and warranties. He is a fellow of the Litigation Counsel of America and can be reached at rbarton@bartonesq.com. **Kenneth N. Rashbaum** (R) is a partner with the firm in New York City, where he leads the privacy and cybersecurity group, advising companies in the areas of data privacy, cybersecurity, information management, information safeguards in service and license agreements, and in litigation and regulatory proceedings. He is an adjunct professor of law at Fordham Law School and the author of articles on topics such as cyber litigation, cross-border transfer of personal information, and HIPAA compliance regarding electronic health information. He can be reached at krashbaum@bartonesq.com.

This article was first published on Reuters Legal News and Westlaw Today on May 16, 2022.