GLOBAL KNOWLEDGE BRIEF

Cybersecurity in 2022

Part 1: How the new SEC proposals could change the game

The Institute of Internal Auditors

Contents

About the Experts

Andy Watkin-Child

Watkin-Child is a 20-year veteran of cybersecurity, risk management and technology, and co-founder of The Augusta Group, a solutions provider for the management, oversight, and assurance of cybersecurity and cyber risk. He has held international leadership positions in 1st and 2nd Lines of Defence (LoD) for cybersecurity, cyber-risk management, operational risk, and technology, working with leadership teams of companies with balance sheets over €1 trillion across the engineering and manufacturing, financial services, and publishing and media industries. He is an experienced member of management boards, global risk leadership teams, and cybersecurity, operational risk, and GDPR committees.

Manoj Satnaliwala

Satnaliwala is chief audit executive and SVP of internal audit for Caliber Home Loans and is responsible for all audit activities, working directly with the audit committee. Prior to his current role, he led the audit function for Radian Group Inc., the third-largest publicly traded mortgage insurer in the United States, and was a director of internal audit for PwC, where he managed the validation of controls for internal audit as part of the CCAR project for a large bank holding company.

Introduction

New regulatory proposals could have huge implications

The news cycle in 2022, and in fact, the last several years, has seen little positivity, and cyber threats have loomed large in a mix that includes the Ukraine crisis, persistent COVID-19 threats, and growing U.S.-China tensions. Together, these variables and more have combined to give cybersecurity a significant — and indeed a leading — spot on internal auditor risk maps.

However, 2022 has also seen cybersecurity-related developments that promise to impact a broad spectrum of organizations, will require more effort to understand, and whose implications will take time to fully grasp. Chief among these are two regulatory proposals from the U.S. Securities and Exchange Commission (SEC). The second proposal is particularly worthy of note because it would require publicly traded businesses that operate in the U.S. to disclose their cybersecurity policies, procedures, and governance strategies, as well as the board's knowledge and experience — if any — in the cybersecurity realm. If implemented (as they are likely to be in some form), publicly traded organizations, regardless of industry or size, will be subject to these new rules. Without hyperbole, these developments represent a new chapter for cybersecurity and a new — if familiar — topic for the internal audit community, which will play a critical role in navigating their organizations through this challenge.

Although this is not a challenge to be taken lightly, internal audit fortunately understands the tools and skills it needs to provide assurance over this evolving risk area. Part 1 of The IIA's three-part Global Knowledge Brief series on cybersecurity presents an overview of the new SEC proposals, including the implications they have for cybersecurity reporting regulation in the U.S. as well as abroad. It also explores how internal auditors can play an important role in helping their organizations manage an altered compliance landscape that new regulations could soon create.

Setting the Stage

Cybersecurity dominating the risk landscape

The top risk of our time

Cybersecurity remains top of mind at all levels of all organizations in all industries in 2022, and that concern is clearly reflected in data from The IIA's *2022 North American Pulse of Internal Audit* (*Pulse*)[1]. When asked to rate the level of risk for their organizations among 13 major risks, internal audit leaders responding to the Pulse survey ranked technology-related risks among the top three — cybersecurity, IT, and third-party relationships (which often include IT services). Even among these top three, cybersecurity easily took the top spot, with 85% of respondents rating it as a high or very high risk, 24 percentage points higher than ratings for IT, the second-highest-rated risk.

Such concern is warranted. In 2021, cyberattacks of nearly every kind increased by alarming margins. According to the *2022 SonicWall Cyber Threat Report*[2], the number of encrypted threats in 2021 spiked by 167% (10.4 million attacks), ransomware rose by 105% (623.3 million attacks), cryptojacking (attacks on computers to mine cryptocurrency) rose by 19% (97.1 million attacks), intrusion attempts rose by 11% (5.3 trillion attacks), and malware directed at the Internet of Things (IoT) rose by 6% (60.1 million attacks).

What's more, all these attacks carry a significant cost for the damage they inflict. The total annual costs of cyberattacks are expected to reach $10.5 trillion by 2025, an average growth of 15% year-over-year, according to the latest version of Cisco/Cybersecurity Ventures' 2022 Cybersecurity Almanac[3].

And this doesn't even factor in the dramatic changes to the geopolitical landscape that impact cybersecurity. Even before Russia's invasion of Ukraine, there was ample evidence that suspected state-sponsored cyberattacks, with high levels of sophistication, were increasing in impact and frequency. The 2020 breach of Texas-based SolarWind's systems, which was conducted by a hacking group reportedly[4] directed by the Russian Foreign Intelligence Service, saw the digital infrastructure of up to 18,000 customers[5] — including Microsoft, Cisco, Intel, Deloitte, parts of the Pentagon, the U.S. Department of Homeland Security, the Department of Energy, and the National Nuclear Security Administration — compromised and undetected for months.

In 2021, another major suspected state-sponsored attack on a U.S. company was seen on the Colonial Pipeline Co.[6] The attack temporarily disrupted the flow of nearly half the gasoline and jet fuel supplies to the East Coast. Ultimately, Colonial paid a ransom of nearly $5 million to hacking group DarkSide to restore the network and recover the data.

1. The IIA, *2022 North American Pulse of Internal Audit*, March 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/
2. SonicWall, *2022 SonicWall Cyber Threat Report*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.
3. Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Cisco, January 19, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.
4. Joe Hernandez, The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says," NPR, updated October 25, 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.
5. Isabella Jibilian and Katie Canales, "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," Business Insider, updated April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.
6. Andrew Marquardt, "As Biden Warns of a Russian Cyberattack, What Are the Precedents? Here's What Happened When a Major Oil Pipeline Was Hacked Last Year," Fortune, March 22, 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

Geopolitical breaking point

Since these attacks, concerns regarding Russia have only escalated, reaching a peak with the invasion of Ukraine. Indeed, Russia's aggression against Ukraine includes cyber warfare — a large-scale attack on Ukraine's power grid[7] — in addition to traditional warfare, and there is increased concern Russia could retaliate against myriad economic sanctions placed on it by the NATO and the U.S. Just one week before Russia's formal move into Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) issued a rare "Shields Up[8]" statement warning U.S. businesses of all sizes to adopt a heightened posture regarding cybersecurity and the protection of critical assets. "Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing," CISA wrote in a March 2022 statement[9] assessing Russian cyber threats.

In May 2021, President Biden signed an executive order[10] designed to improve the state of national security in the U.S. The order specifically addressed the need for government agencies to review and develop new guidelines and standards for cybersecurity, and for organizations to focus on enhancing software supply chain security and threat information sharing. More recently, the President also issued a statement reiterating the Russian cybersecurity threat and highlighting CISA's evolving guidance[11] on the subject.

Russia is not the only state actor allegedly backing destabilizing cyberattacks. According to a 2021 report[12] from The Evanina Group, China has become increasingly aggressive on the cyber front, especially in regard to data acquisition of personal information and data privacy.

"China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed," said William Evanina, former director of the National Counterintelligence and Security Center.

Evanina referenced numerous cyber incidents linked to the Chinese Communist Party, including the 2017 Equifax cyber breach; a 2011-2018 campaign by four Chinese nationals to hack into dozens of companies, universities, and government entities; and a 2011-2013 state-sponsored cyber campaign attacking U.S. oil and natural gas pipeline companies (the DOJ released a report on this incident in July 2021). He also referred to a July 2021 report from the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and CISA that released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the U.S.

It is in this complex and overall dangerous cyber environment that the SEC has taken historic steps to address cyber health and preparedness across the organizational landscape, particularly in regard to reporting to the SEC and (in some cases) the public. Such steps are the first of their kind, and could have significant implications not just for publicly traded U.S. companies but companies across the globe.

7. IANS, Ukraine Foils Russia-backed Cyber Attack on Power Grid," April 14, 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.
8. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up," accessed April 22, 2022, https://www.cisa.gov/shields-up.
9. Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," Department of Homeland Security, accessed April 22, 2022, https://www.cisa.gov/uscert/russia.
10. U.S. General Services Administration (GSA), "Executive Order 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.
11. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up."
12. William Evanina, "Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP), The Evanina Group, August 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

The Big Change

A historic first step toward cyber incident disclosures

The proposals

Within a two-month span, the SEC unveiled two long-anticipated proposals addressing cybersecurity in the business sector. The first proposal[13], revealed in February 2022, focuses on registered investment advisers, registered investment companies, and business development companies or funds. Under the proposed rules, advisers and funds would be required to:

- Adopt and implement written cybersecurity policies and procedures designed to address cybersecurity risks that could harm advisory clients and fund investors.
- Report significant cybersecurity incidents affecting the adviser or its fund or private fund clients to the SEC on a new confidential form.
- Publicly disclose cybersecurity risks and significant cybersecurity incidents that occurred in the last two fiscal years in their brochures and registration statements.

Additionally, the proposal would set forth new recordkeeping requirements for advisers and funds designed to improve the availability of cybersecurity-related information, as well as help facilitate SEC inspection and enforcement capabilities.

"Cyber risk relates to each part of the SEC's three-part mission, and in particular to our goals of protecting investors and maintaining orderly markets," said SEC Chair Gary Gensler in a press release[14]. "The proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks."

While these rules reflect — if implicitly — SEC expectations for how regulated entities should manage cybersecurity risks and report cybersecurity incidents, the second proposal makes such expectations explicit. Directed at all publicly traded companies, the second proposal[15], issued in March 2022, seeks to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934." To do so, the new rules would require public companies to provide disclosures regarding:

- The company's policies and procedures to identify and manage cybersecurity risks. Included with the rules is an extensive but non-comprehensive list of risk management strategies, policies, and procedures that may be subject to disclosure, including:
    - Whether the registrant has a cybersecurity risk assessment program.
    - Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program.

13. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," February 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
14. U.S. Securities and Exchange Commission (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9, 2022, https://www.sec.gov/news/press-release/2022-20.
15. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- Whether the registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider.
- Whether the registrant undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents.
- Whether the registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.
- Whether previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies.
- Whether cybersecurity-related risks and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition.
- Whether cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation.

- Management's role in implementing cybersecurity policies and procedures, including:
  - Whether certain management positions or committees are responsible for measuring and managing cybersecurity risks.
  - Whether the registrant has designated a chief information security officer or someone in a comparable position.
  - Whether processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.
  - Whether such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risks, as well as how frequently they report.
  - Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks.
  - Whether the board is informed about cybersecurity risks and the frequency of its discussions on such risk.
  - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

- The board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risks. This includes information on:
  - Whether the board has work experience in cybersecurity.
  - Whether the board has obtained a certification or degree in cybersecurity.
  - Whether the board has knowledge, skills, or other background in cybersecurity.

Additionally, the proposal includes an amendment to Form 8-K, which would require public companies to disclose cybersecurity incidents within four business days, just as they are already required to do for any other unscheduled material event. Such disclosures would include:

- When the incident was discovered and whether it is ongoing.
- A brief description of the nature and scope of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.
- The effect of the incident on the company's operations.

- Whether the company has remediated or is currently remediating the incident.

These disclosures, according to the SEC, would provide investors with "consistent, comparable, and decision-useful" information. "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend," said Gensler[16]. "The interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data are only accelerating, putting our financial accounts, investments, and private information at risk. Investors want to know more about how issuers are managing those growing risks."

The historical significance

In many ways, the structure of these described rules mirrors other SEC disclosure rules, such as those related to financial conditions and operating results (Sarbanes-Oxley), insider information, and organizational strengths, weaknesses, opportunities, and threats. However, taking the additional step of elevating cybersecurity risks to point of necessitating such disclosures is largely unprecedented.

"The U.S. is probably the first country, and I would say only country, in the world to regulate cybersecurity," says Andy Watkin-Child, founding partner of The Augusta Group and Parava Security Solutions, and the founder of Cybersecurity Maturity Model Certification Europe (CMMC Europe). "Companies in the U.S. may be familiar with the EU's General Data Protection Regulation (GDPR) and may be quick to group these proposals together, but data protection and cybersecurity are two different paradigms. There's a big difference, and other than arguably the Department of Defense (DoD) Financial Management Regulation — which could result in even foreign contractors getting investigated by the Department of Justice for cybersecurity vulnerabilities — there's nothing else like it in the cybersecurity realm."

Watkin-Child also explains how the significance of the new rules could have strong ripple effects abroad. "The Ukraine crisis has proven that cybersecurity is a weapon, and indeed NATO has considered it a degree of operation since 2016," he says. "Cybersecurity is an offensive tool right alongside nuclear weapons. The problem with that is because it's a domain of operation, it poses a grave threat to national infrastructures. The SEC proposal is hitting the big players first — the trading firms — but my belief is that this will hopefully trickle down into organizations beyond SEC purview because the business landscape, as well as the federal landscape, is so intertwined on a global level."

In war, says Watkin-Child, one cannot consider cybersecurity within just a single military; if one ally is vulnerable, that has a direct effect on the entire joint operation. Cybersecurity protection for public — and private — companies is no different. "If American weapons systems can't get hacked while British systems can, there's no point in having protection at all," he says. "There's a reason the [U.S.] president has spoken to NATO regarding, among other things, common cybersecurity standards. It's the right thing to do, because if an entity like Russia uses the business sector to attack power generators, for example, your water, your electricity, your gas, your healthcare — it's all gone."

Such potential consequences are obviously macro in nature, but it is important not to discount organization-level consequences, as well. And despite what one might feel seeing the extensive lists of elements that could warrant inclusion in cybersecurity disclosures, not all the consequences are negative.

"Of course, there's the legal side to the disclosures," says Watkin-Child, "But, as it states in the proposals, you're not just reporting to the SEC. You are reporting to all the market participants who might have an impact on your business. The investment community, credit rating agencies, insurance companies — they are all going to see alongside the SEC how good you are at cybersecurity, or not, as the case may be. Such transparency comes with risk, but it also represents an opportunity."

16. Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," U.S. Securities and Exchange Commission (SEC), March 9, 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

Internal Audit's Role Remains Consistent

Identify, assess, communicate

The tools are in place

The Sarbanes-Oxley Act of 2002 (SOX) provided additional responsibilities and unlocked new opportunities for internal audit functions to add value to their organizations. Indeed, as organizations navigated the new legislation, internal audit to many became synonymous with SOX compliance. Due to the nature of the new SEC proposals, there is cause to believe the same could happen in the realm of cybersecurity.

At first blush, this may seem like at least a short-term impossibility due to the complex nature of the cybersecurity field. According to Pulse survey[17] respondents, cybersecurity makes up on average just 9% of audit plan allocation in publicly traded organizations, which is up from 7% the previous three years but far below the 35% allocated for financial reporting. There are several reasons why this might be, such as budget limitations, lack of sufficient resources, and lack of knowledge or experience.

The real value internal audit can provide, however, is not necessarily through cybersecurity knowledge, but knowledge of risk identification, communication of risk, and the evaluation of controls to address risk. Indeed, these are the very things the SEC proposals wish to emphasize for one specific risk.

"It's important to realize that these proposals are not really about cybersecurity, they are about cybersecurity risk management," says Watkin-Child. "When people think cybersecurity, they all think about implementing controls and fixing stuff. What the SEC is looking for is something completely different; they're looking for organizations to assess their cybersecurity risks. They want boards in organizations to have the governance structures in place to evaluate and assure oversight of their cybersecurity risk management program, whatever form it may take."

"What the SEC wants to see is boards taking responsibility for oversight and assuring the rest," says Manoj Satnaliwala, chief audit executive of Caliber Home Loans, Inc. "The gap isn't really in cybersecurity standards — there are frameworks in existence to guide organizations, such as the NIST Cybersecurity Framework. The real gap is in accountability, which can quickly become a responsibility seesaw."

The role of internal audit can help bring balance to this seesaw. "Boards and management, they need help. Internal audit through assurance ensures accountability and, through enhanced visibility across the organization, promotes shared risk ownership," says Satnaliwala. "The risk is different, but the role of internal audit really remains consistent. Audit functions don't have to start fresh, and it's unreasonable to expect every internal audit shop to be in the nitty-gritty of a cybersecurity program, but in regards to this challenge, it's little more than looking at the SEC proposals and asking, 'What are the SEC's expectations?' As long as there are at least some cybersecurity resources already in place, I don't think any changes are needed in the average internal audit function other than tweaking approaches to ensure proper risk coverage."

However, having access to such cybersecurity resources is often easier said than done. Developing any degree of expertise in cybersecurity through training and certifications will not happen overnight, and especially for small internal audit functions with limited budgets to recruit costly, high-demand talent, options to perform any kind of role beyond process-driven compliance is limited. In these cases, internal audit must have a comprehensive understanding of where the knowledge can best be accessed. This can be:

17. The IIA, 2022 North American Pulse of Internal Audit,"

- **Within the organization's own talent base.** Those with experience in a more traditional IT audit capacity often have the knowledge base to complete technical cybersecurity training relatively quickly. Additionally, certain cybersecurity fundamentals can be incorporated into areas such as change management, access controls, IT operations, and disaster recovery, which could reduce the need for outsourcing long term.
- **Through collaboration with both the second line and trusted external audit functions.** While internal audit's independence and objectivity must be maintained in conformance to the *International Standards for the Professional Practice of Internal Auditing* (IPPF), establishing a more collaborative working relationship with relevant functions such as IT can provide auditors with indirect access to technical competencies that otherwise may be difficult or costly to obtain.

Conclusion

Time to prepare

Cybersecurity, as a subject, is always evolving as bad actors continue to innovate in their approaches and companies continue to innovate to thwart them. However, as the history of cybersecurity continues to be written, 2022 will be remembered for the milestones reached in an effort to counteract the dire trends seen across the business landscape. Although the SEC proposals must both complete a 60-day period for comments before official rules are issued, there should be little in the way of surprise for publicly traded companies and their internal audit functions.

Internal audit can and should use the time it has, if it has not already done so, to take stock of the full scope of the assets of its organization that should be accounted for in a cybersecurity strategy. Without that knowledge, internal auditors will find it difficult to assess whether current cyber-related controls, policies, and governance strategies are sufficient. Such assessments are not just important for organizational security purposes, but indeed for the entire market community. The world is becoming more interconnected by the day, and this means responsibilities regarding risks such as cybersecurity are largely shared. After all, as history has shown time and again, the breach of one organization could have a very real impact on the security of another.

A chain is only as strong as its weakest link.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 210,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit theiia.org.

Disclaimer

Copyright

April 2022

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101