Cybersecurity Is a Growing Focus for the SEC and Military

The SEC's new cybersecurity rule spells out how U.S. companies will need to battle cyber threats, while the U.S. military is feeling the pressure to launch a new branch to fight in cyberspace. AI could be part of the solution—and part of the problem.

Erik Swords
Lead Portfolio Manager

Key takeaways

- The SEC is requiring publicly traded companies to do more—and tell investors more—about the cyber threats they face. We expect this will result in increased spending on all aspects of cybersecurity.
- Whether or not the U.S. military builds a dedicated "Cyber Force," it has been laser-focused on this problem since 2009, when it launched the intra-agency United States Cyber Command.
- The market for AI-based cybersecurity products is estimated to reach $133.8 billion by 2030, but criminals have also been using AI-based technologies to launch more sophisticated attacks.

Individuals and organizations everywhere are grappling with data breaches, online crime and a growing dependence on artificial intelligence (AI). This is pushing cybersecurity issues to the fore, and two notable developments are worth a closer look: a new SEC rule and a proposed new U.S. military branch.

In the news: New SEC rule heralds a tougher approach to cybersecurity

On December 10, 2023, the Securities and Exchange Commission (SEC) will implement a new rule requiring public companies to disclose material cybersecurity incidents and cybersecurity risk management, strategy and governance. There are three key parts to this rule.

Exhibit 1: Attacks are happening faster than organizations can respond
Average time between compromise of systems and exfiltration of data

Source: Palo Alto Networks, Unit 42 Cloud Threat Report—Volume 7. Data as of 2023.

- Companies must **take a more proactive approach** to cybersecurity risk management, developing and implementing comprehensive programs designed to identify, assess and mitigate cyber risks.
- Companies must **disclose material cybersecurity incidents to the SEC within four business days** of discovery. Currently, it takes five days (or even less) for attackers to "exfiltrate" data from a company's systems (see Exhibit 1), and about six days for companies to remediate the attacks. Industry advances—including a greater integration of AI—have brought this remediation number down in recent years. Yet the SEC rule still results in a significantly quicker response than is the case today. This means that companies will need to have a process in place for quickly detecting and investigating cybersecurity incidents.
- Companies must **disclose more information in their 10-K filings** about their cybersecurity risk management, strategy and governance. Investors will be able to study these annual financial reports to assess a company's cybersecurity posture and make informed investment decisions. It will also call attention to companies with insufficient cybersecurity measures in place. We expect this will result in increased spending on perimeter, network, endpoint, application and data security.

Some investment analysts have suggested that the SEC's new rule is one of the most important cybersecurity policies in history,[1] further raising the priority and budget focus on security. We see a few immediate implications.

- **Increased compliance costs:** Companies will need to invest in new resources and technologies to comply with the new rule. This could include hiring additional cybersecurity staff, implementing new security controls and conducting regular risk assessments.
- **Increased regulatory scrutiny:** The SEC will be more closely scrutinizing companies' cybersecurity practices. This could lead to increased enforcement actions against companies that fail to follow the SEC's guidance.
- **Greater risk of reputational damage:** A cybersecurity incident can damage a company's reputation and financial performance, and the new rule will make it more likely that cybersecurity incidents will be made public.
- **Increased shareholder activism:** Shareholder groups are increasingly focused on cybersecurity risks. The new rule could lead more shareholders to demand that companies improve their cybersecurity practices.

[1] Morgan Stanley, 07/26/23.

In the news: Should the U.S. military launch a "Cyber Force"?

The U.S. military owns some of the world's most sensitive data and has been highly focused on the issue of cybersecurity for years. Yet so far, **each branch of the military deals with cybersecurity separately.** There is some level of coordination via the United States Cyber Command, the military's digital warfighting arm consisting of members from multiple military branches and other government agencies. Yet some critics say this is a piecemeal and insufficient approach, particularly considering that digital threats from China, Russia, North Korea and others have only multiplied since Cyber Command was established in 2009.

The result is "inconsistent readiness and effectiveness," according to the Military CyberProfessional Association (MCPA), a contingent of current and former military leaders that boasts around 3,700 members. In May 2023, **the MCPA urged the U.S. Congress to establish a separate division focused on cybersecurity.** They are calling for a dedicated branch of the military to tackle the increasing nature of cyber challenges with an active approach. If adopted, **a "Cyber Force" would be established alongside the Army, Navy, Air Force, Marine Corps and Space Force.** So far, the response from military leaders and government officials has been mixed. Critics point to the fact that the current Cyber Command is already viable and well-entrenched—and that it's a bad time to reorganize in the face of rising cyber challenges.

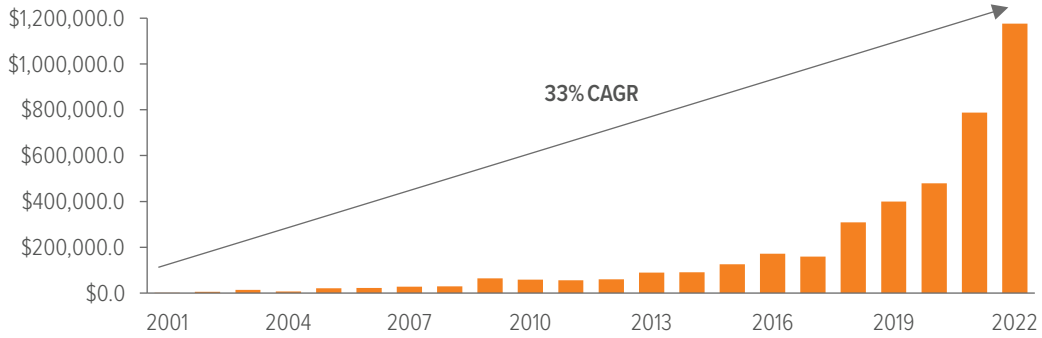
> **"Only a [separate branch of military] service, with all its trappings, can provide the level of focus needed to achieve optimal results in their given domain. Cyberspace, being highly contested and increasingly so, is the only domain of conflict without an aligned service. How much longer will our citizenry endure this unnecessary risk?"**
>
> —Memorandum from the Military CyberProfessional Association urging the U.S. Congress to establish a U.S. Cyber Force in the 2023 annual defense policy bill.

Why it matters

The **SEC and U.S. military's increasing focus on cybersecurity** shows just how much the world is vulnerable to cybercrime—particularly with the growing use of generative AI, the internet of things (IoT) and cloud computing. Amid soaring financial losses (Exhibit 2), **the cybersecurity market is expected to grow at a rapid rate** (Exhibit 3).

Exhibit 2: Global financial losses from cybercrime grew 570x since 2001

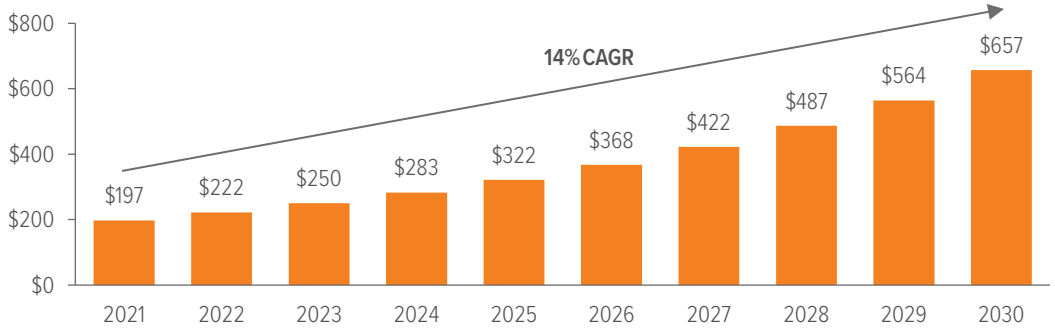
Hourly financial losses ($)



As of 04/23. Source: Surfshark Research. CAGR = compound annual growth rate.

Exhibit 3: Global cybersecurity market expected to reach $657 billion by 2030

Market revenue ($ billions)



As of 08/23. Source: Statista; Next Move Strategy Consulting. 2023-2030 figures are estimated.

AI is playing a critical role in cybersecurity, for good and bad, with many companies employing the latest AI-based cyber tools to better secure their systems and data. The global market for AI-based cybersecurity products is estimated to reach $133.8 billion by 2030, up from $14.9 billion in 2022.[2] However, criminals can also use AI-based technologies to launch more sophisticated attacks. For example, AI-developed phishing emails are opened more frequently than manually developed versions, leading to greater losses for consumers and companies.

Another solution involves bolstering the ranks of skilled cyber professionals who can address these issues—but the demand is outpacing supply, posing significant risks to organizations worldwide. According to a recent survey by the International Association of Privacy Professionals, 59% of organizations struggle to find qualified cybersecurity professionals. Addressing these challenges will require a concerted effort from governments, educational institutions and the private sector to ensure that the cybersecurity industry has the talent it needs.

[2] Acumen Research and Consulting, 07/22.

VOYA® INVESTMENT MANAGEMENT