Boardroom Takeaways: 2022 Vulnerability Intelligence Report

The threat landscape today is radically different than it was even five years ago. The flourishing cybercrime ecosystem is complex, diverse, and reliably profitable at the expense of global corporations. Ransomware groups and initial access brokers have joined botnet operators and state-sponsored threat actors in growing a cybercrime economy whose wide-ranging tactics and targets leave virtually no organization unsqueezed, irrespective of size or vertical.

A persistently elevated threat climate

- 2021 marked an all-time high for cyberthreat speed and scale, with mass exploitation events occurring every 11 days on average. 2022 saw a modest dip in zero-day exploitation and mass exploit "outbreaks," but the multi-year trend of rising attack speed and scale remains strikingly consistent overall.
- As cybercrime business models and attacker behaviors evolve, we expect to keep seeing minor fluctuations in year-over-year macrotrends. Notably, while this variability gives rise to nuanced analysis of adversaries and their motivations, it does very little to temper the persistently elevated risk climate for global businesses.

Mature cyberthreat operations often outpace security teams

- We continue to see a shortened window between when new vulnerabilities are discovered and when they become leveraged in attacks. In 2022, 56% of the vulnerabilities in our report were exploited within seven days of discovery, and more than 40% of widespread attacks began with a zero-day exploit. This means security teams have a steadily shrinking or simply non-existent window to patch new vulnerabilities and prevent successful attacks, which puts considerable strain on the already stretched security resources of many organizations.
- Having a well-developed emergency patching procedure as well as a generally robust incident response procedure is beneficial. But it is not realistic to expect teams that are still struggling with resourcing for foundational security program activities to have strong emergency procedures in place. Security teams need to be able to implement robust security program basics, like proactive asset and vulnerability management practices, before they can respond effectively to a crisis.

Technology requires expertise to be effective

- As cloud adoption expands and technology stacks become ever more complex, available attack surface also grows, offering adversaries more ways to compromise corporate networks. Technological solutions are a necessary component of any organization's security posture, but

combating and preventing modern cyberthreats almost always requires human expertise in addition to technologies that deliver visibility and protection across the entirety of a company's cloud and on-prem footprint. Business leaders should not assume technology alone is an adequate solution to complex attack patterns, and should evaluate their organizational ability to implement security frameworks that detect and deter motivated adversaries.

Advice for the C-Suite and Boardroom

- In today's threat landscape, security teams are frequently forced into reactive positions, lowering security program efficacy and sustainability. Boards and executives benefit from gaining visibility into the challenges security programs face and the potential impact of their deterioration.
- Challenging macroeconomic conditions in 2022 and 2023 have put further pressure on risk management teams as they look to drive efficiencies without compromising the integrity of sensitive data or business operations. Particularly in a volatile macroeconomic climate, ongoing resource constraints can lead to hidden risk accumulation and loss of technical expertise required for effective security operations, including emergency incident response capabilities.
- Business leaders should recognize the increasingly widespread nature of security threats and the ubiquity of both sophisticated and commodity attacks on corporate networks. Security metrics and organizational risk models should be informed by business context and incorporated into broader strategic planning activities. Optimally, security should be considered a company-wide responsibility that is not owned solely by isolated functional areas.
- An acceptable risk is an articulated risk: Boards and C-level executives should have a full and communicable understanding of how security program resource constraints and the realities of the threat climate may affect the continuity of business operations — including confidentiality of intellectual property and the integrity of sensitive data and supply chains. It is fundamentally reasonable for boards and the C-suite to accept risk as part of business decision making, as long as that risk is contextualized and explicit.