ANALYST CONNECTION

Sponsored by: GoSecure

While security spend will remain largely resilient, security investments are under scrutiny. The growing strategic importance of cybersecurity will get the attention and involvement of CEOs and business executives.

The State of Cybersecurity Today in Light of the Current Threat Landscape and Economic Uncertainty

October 2023

Questions posed by: GoSecure

Answers by: Cathy Huang, Research Director, Security Services Worldwide

Q. What is happening in the cybersecurity field today?

A. There is no doubt that cybersecurity has grown in strategic importance over the years. Over the past two decades, organizations have increased their reliance on technology in efforts to improve their customer experience, business operations, supply chain management, employee productivity, and so forth — essentially using technology to achieve their competitive advantage. During the COVID-19 pandemic, for example, organizations used digital technologies and infrastructure effectively to support the proliferation of remote workers. IDC research shows that 49% of organizations noted productivity increases of up to 24% due to investments in digital transformation. In fact, many technology leaders have been praised for their efforts to provide the essential availability and resilience to maintain critical business continuity.

However, digital transformation has not been without its challenges. For instance, remote work and increased cloud adoption significantly increase the attack surface and introduce vulnerabilities latent in the home or remote network. Similarly, IT organizations lack visibility into many of the devices on the enterprise network that introduce new cybersecurity risks. As a result, cybersecurity risk is mounting rapidly, resulting in costly data breaches, disruptions, and damages to the business.

Cybersecurity trends have become much more relevant as digitally transformed businesses realize that their very existence may depend on their capabilities to withstand a cyberattack and quickly restore to a viable operating status. In a year like 2023, many organizations face unprecedented financial stress due to inflation and economic uncertainty. While security spend will remain largely resilient, security investments are under close scrutiny. CEOs and business executives now expect clear metrics and measurement of results to assess and validate investments made in their organizations' security programs.

Q. How does the current threat landscape differ from the past, and what does the future hold?

A. The number of threat actors continues to grow as there are real rewards to be had, whether monetary gains, corporate espionage, or economic advantage from state-sponsored actors. In addition to financially motivated cyberattacks, the rise of geopolitical tensions has led to a surge of politically motivated hacktivist attacks.

IDC has been tracking ransomware activities since the first half of 2021. Since July 2021, we can clearly see that the sheer number of ransomware attacks across the world has grown significantly, as have the associated payments. The increasing rate of digitalization has significantly expanded attack surfaces as well as exposed deficiencies in legacy security practices and reactive security strategies. For instance, the series of VMware ESXi ransomware attacks in February 2023 that impacted over 3,800 servers had exploited a two-year-old vulnerability. It turns out that many customers were running out-of-date or unpatched versions of the VMware ESXi software.

Ransomware continues to be a borderless threat that shows no sign of letting up in 2023. The ransomware landscape has become more complex and advanced as threat actors constantly find new ways to operate. One of the most notorious ransomware groups, LockBit, has been rebranding and restructuring its affiliate organization after years of bad press. The ransomware group even introduced the first bug bounty program, with incentives of up to $1 million for vulnerabilities it can exploit. Its latest malware, LockBit 3.0, is able to self-propagate or spread through the victim network entirely without human intervention.

Ransomware is just the tip of the iceberg when considering the entire heightened threat landscape. APTs, phishing, data breaches, business email compromise, denial of service, and other cyberattacks have become commonplace. One of the most worrying developments is the increase of malicious cyberactivities targeting industrial systems (e.g., Industroyer malware), posing a significant threat to vital services that sustain our daily lives. There is a catastrophic possibility that the world is facing a "COVID-19"-like major cyberincident where an adversary leverages artificial intelligence (AI) and GenAI tools to engineer much more sinister cyberattacks capable of causing unprecedented harm.

Q. What will the cybersecurity field look like given the current economic landscape and the obstacles organizations face due to a worsening economy?

A. While the overall economy is unpredictable, many CEOs are gearing up to continue investing in their organizations' digital business strategy. In IDC's annual *CEO Sentiment Survey* conducted at the beginning of 2023, 87% of surveyed CEOs across the world stated that they are looking to sustain or increase technology spending in 2023. Moreover, "security, risk, and compliance" is identified as the technology area most immune to budget cuts in 2023. This indicates that cybersecurity threats and compliance issues, which have been top-of-mind concerns, are seen as the most important business risk for CEOs.

However, with macroeconomic headwinds that project an economic slowdown swirling about, companies cannot afford to increase the security spend at the rate of their digital transformation process. What's more, risk exposure increases the

longer organizations take to decide what to spend and where, as well as the lower the security budget. What is not helping organizations is the lack of available cybersecurity talent. This shortage continues to be a top challenge and is not forecast to subside any time soon.

Every organization has a different risk profile as well as risk appetite. This variable stance on risk is the result of an organization's specific industry sector as well as geographic presence. An organization's approach to risk often also determines the organization's investment priorities. Take as an example the tech layoffs and restructuring occurring in recent months. Some CEOs may become more hesitant to spend money on new projects given the uncertain economic outlook. However, there are other CEOs who may see the current situation as an opportunity to invest in key areas and new technologies like artificial intelligence and machine learning (ML) to give their businesses a competitive advantage.

Q. Given the dynamic nature of cybersecurity, how can organizations plan and prepare for tomorrow?

A. Organizations of all sizes, and especially small to medium-sized businesses, struggle to build cost-effective and future-proof cybersecurity programs. To address the pain points and the many issues faced by the modern digital business, organizations need a customizable, integrated, and future-proof cybersecurity program that enables a strong cybersecurity posture, supports cyber-resilience, and helps meet cybersecurity and compliance objectives in a cost-effective manner. This involves a holistic program that includes many security solutions with the ability to integrate into the existing IT infrastructure, along with the appropriate staffing to configure, maintain, and manage the solutions.

An integrated cybersecurity program requires a comprehensive approach that covers multiple aspects of security domains and technologies. For example, a well-functioning security monitoring system offers broad endpoint and network visibility, enabling the collection of security signals and telemetry to improve the efficacy of incident detection tools. At the same time, elimination of security silos reduces time to detection of destructive threats such as ransomware, as well as insidious insider threats, reconnaissance, and data theft.

In IDC's latest worldwide security services primary research survey conducted in February 2023 (with a total sample size of 1,214 organizations across the world), 61% of all respondents indicated they have a cyber-resilience strategy in place and have deployed related technologies across functions. However, only 20% of them would regularly test their cyber-resilience plan. If the plan is hardly tested or just a static document without the ability to incorporate the lessons learned, the effectiveness of the cyber-resilience plan is questionable.

Q. How do future cybersecurity trends factor into the forecast of cybersecurity strategic planning?

A. Prior to the enthusiasm around generative AI, the cybersecurity field had used different kinds of artificial intelligence, machine learning, and predictive analytics for a while. In *IDC FutureScape: Worldwide Future of Trust 2023 Predictions* (IDC #US49755022, October 2022), the first prediction is about autonomous security operations centers (SOCs): "By 2026, 30% of large enterprise organizations will migrate to autonomous security operations centers."

The power of leveraging multiple integrated and coordinated platforms that gives organizations automated insight into architecture, threats/vulnerability, risks, policies, and standards will be tremendous. Autonomous SOCs can provide insight into threats that might be missed by an overworked and fatigued cybersecurity team or are beyond traditional defenses. IDC believes that large enterprise organizations, especially those with significant cloud-based systems, will consider investment in autonomous SOCs to aid their existing cybersecurity workforce.

In the near term, expect the use GenAI to facilitate the trend of the autonomous SOC because what underpins the autonomous SOC is the reliance on AI/ML used in security detection, orchestration, automation, and response. For instance, organizations can use AI/ML to continuously scan the threat landscape for new and emerging threats, which promises to identify, triage, and remediate threats at scale.

Moreover, the use of GenAI will bring significant changes to the user interface between the user and an autonomous SOC platform. GenAI focuses on a set of unsupervised and semi-supervised foundational models that create new content from previously created data such as text, audio, images, and code. The rapid adoption of GenAI will move AI from a nascent software element in the tech stack to a linchpin technology at the center of a platform transition toward AI everywhere.

About the Analyst

Cathy Huang, *Research Director, Security Services Worldwide*

Cathy Huang is a research director in IDC's Security and Trust research practice focused on managed security services, security consulting, and integration services within the security services program. In addition, she collaborates with other team members to look at services that help organizations adopt emerging technologies like edge, 5G, and IoT as well as key focus areas such as cloud security, cyber-resilience, and cybertransformation.

MESSAGE FROM THE SPONSOR

GoSecure

GoSecure is a recognized cybersecurity leader, delivering Managed Extended Detection and Response (MXDR) solutions and professional services. For over 10 years, GoSecure has been helping customers better understand their security gaps, improve organizational risk, and enhance security posture through advisory services provided by one of the most trusted and skilled teams in the industry. Learn more about how GoSecure's MXDR solutions ensure organizations are well-equipped to navigate the ever-changing threat landscape.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com