IDC ANALYST CONNECTION

Sponsored by: Micro Focus

Shift left, be strategic, and iterate. These are the core principles of cyber-resilience in today's digital business.

Intelligent Outcomes Are Key to Business Resilience

November 2020

Questions posed by: Micro Focus

Answers by: Christina Richmond, Program Vice President, Security Services

Q. In the age of enterprise resilience, what guidance would you offer chief information security officers (CISOs) as they evolve their programs to account for unexpected crises or adversities?

A. Cyber-resilience offers a unique opportunity for the CISO to play a strategic contributing role in enterprise resilience. Cyber-resilience provides a platform for the CISO to enable the organization to pivot and grow during times of adversity (e.g., crisis, pandemic, and even business volatility) by being more agile, adaptive, predictive, and resilient. The benefit of doing so is that the CISO organization will be part of "enabling the business" as opposed to just "protecting the business."

Cyber-resilience can and should be built on an organization's existing foundation, rationalizing and consolidating tools where possible. Increasing resilience does not have to require an architectural lift and shift. A building block approach starts with an inventory of high-value assets (HVAs) and data and then looks to map data flows and define access management. This is assessment work. Assessment leads to strategy definition. Hence, scraping and rebuilding from the ground up is not required, but rethinking the cybersecurity strategy and program is important. In a phased manner, organizations should seek to perform the previously mentioned assessments first and then add advanced analytic technologies and tools to bring to light previously unmined and uncontextualized data. Advanced tools such as user and entity behavior analytics (UEBA), cluster analysis anomaly (looking for discrepancies among groups), and outlier detection can help detect and correlate new sets of data from Internet of Things (IoT) and operational technology (OT) software across hybrid, multiedge, and multicloud environments and thwart cybercriminals while meeting compliance requirements. In addition, they can port to new architectures, whether cloud based, software defined, or hybrid. Such tools are not a panacea for detecting unknown threats, but when they are combined with complementary methods, processes, inspections, and capabilities, an organization has the ability to better address adversities.

Adapting to resilience is a frame of mind as much as it is a technical viewpoint. The collaborative nature of building intelligent outcomes ahead of product development will foster a cross-company lexicon. Security teams must break down silos and listen to stakeholders outside the technical domain. Security, risk, privacy, and compliance have long been obstacles to innovation; technology advancements remove these obstacles. CISOs must strive to be enablers of innovation. Executives and board members should be included not only in the initial innovation phase but also in the planning of response and recovery. What-if testing will highlight security vulnerabilities and compliance gaps and should outline directives to navigate risk appetite. When a breach is detected (whether from security, compliance, or risk outliers), these stakeholders need to know how and when to respond. Building the plan and iterating with this team are imperative for resilience.

Q. What are the key aspects of evolving cybersecurity into more of a cyber-resilient mindset?

A. Long seen as the department of "no," cybersecurity is slowly evolving to enable the business. Fear, uncertainty, and doubt (FUD) industry marketing still exists, but security technologies and personnel are beginning to embrace security by design, least privilege, and security as code. The human brain thinks up tremendous advancements but also gets stuck in the same old rut. Think of the hours security analysts sit in front of a screen playing "whack-a-mole" with cyberadversaries and the sheer number of alerts they attempt to investigate one at a time. Isn't this the definition of insanity? Augmenting analysis with machine brainpower is one way to break out of old ruts and expand human capabilities. Inclusion of algorithmic detection across all types of telemetry furthers the organization's chances against an adversary that may be better funded and tooled. Embracing data science to reduce human burnout and increase mean time to detection of anomalies and events creates the following equation: human + machine = cyber-resilience.

Once upon a time, best-of-breed technology from one vendor promised interoperability, efficiency, better patching, and easier configuration, but today's very distributed landscape requires a broader ecosystem. One-stop shops are limited in the power they wield in today's multifaceted environment. Because of the diversity of network, connectivity, datacenter, and compute options, it's better to partner for best-of-breed technology, operational management, and consultative know-how rather than rely on one tried-and-true product or service provider. Organizations should seek unique domain expertise in industry intellectual property and knowledge and best practices from global partners — practices that are built directly into existing products as controls.

Organizations must think strategically. It is critical to have a 100,000-foot view, then a 30,000-foot view and, finally, a local view of today's reality. It is also key for cyberteams to review strategy and plans and react as fluidly as digital technologies now enable data to move. Moreover, organizations need to iterate. Just as sensors sense continuously, and 5G and edge compute will deliver new industry capabilities, organizations must strive to continuously refresh and evolve their cybersecurity programs.

Q. How do organizations structure their cyberinvestments and cyberstrategies to "shift left" and support business growth and enablement?

A. "Shift left" is a software development practice intended to find and prevent defects early in the programming process. We can learn from the continuous integration and delivery of code changes when we think about strategically investing in our cybersecurity posture. In this light, shift left means improving risk posture and resilience by considering security and risk early in the business innovation life cycle. We do this by considering the business goal, or outcome, as a precursor to investing. Applying intelligent outcomes assists business and technology teams with thinking about protecting and recovering high-value assets and data before and during product development. These outcomes incorporate cybersecurity and necessitate the inclusion of risk, privacy, and compliance.

Intelligent outcomes also require cross-stakeholder collaboration as product scrum teams whiteboard new innovations. C-suite and board members should, at the very least, be consulted in initial whiteboarding sessions because their broader business perspective is central to defining cybersecurity and cyber-resilience goals. CISOs and chief risk officers (CROs) seek to understand whether insider threat risks are introduced when new supply chain and third-party stakeholders join product/service development plans or employees are suddenly distributed outside the corporate network, as we've seen in 2020. Compliance officers must keep an eye on data privacy and regulatory controls. Ultimately, the C-suite and board desire to know that all considerations have been made ahead of development to protect the business.

Q. Why do intelligent outcomes matter, and how might they shape cyber-resilience?

A. The adage "insanity is doing the same thing over and over again and expecting different results" applies well here. In the hyperconnected, sensor-driven world we live in today and expect to proliferate in coming years, legacy cybermethodology is insufficient. We are at an inflection point in technology buildout where changes in digital business will soon outpace (and one could say already are outpacing) changes in the structure of cybersecurity programs, strategies, and operations. Cybersecurity is critical, but true resilience means not only that the core business functions are protected but also that the organization can respond, recover, and get back to business rapidly in the event of a disaster.

Organizations should consider the "what ifs" of security breaches, data loss, and potential loss of brand trust ahead of product development. They should include business as well as technology constituents to promote more thoughtful product and service innovation and, even more critically, to plan for and practice business continuity and disaster recovery (BCDR) scenarios. 2020 will go down in the history books as the year that drove greater digital adoption and cloud migration than any prior year.

It is also the year that saw more agile work-from-home migration by companies well ahead in this technology revolution. Companies that established in the cloud and software-defined infrastructures were lighter on their feet in reducing risk and cybervulnerabilities than their cohorts, which still had to make the shift to digital environments. These earlier adopters must also have had an intelligent outcome in mind ahead of their journey to resilience. They couldn't have known that a pandemic would impact business the way that it has, but they nonetheless planned for infrastructure agility, workload scalability, and modern workforce flexibility. This is where intelligent outcomes can help determine ultimate resilience.

Q. What are the biggest areas of cyber-resilience innovation and enablers to drive overall enterprise resilience?

A. Security technology bloat has caused inertia, which is exactly the opposite of what was intended. But this is changing. Machine learning, artificial intelligence, and automation increase the speed of detection and investigation of cyberattacks. Likewise, software-defined architectures, network segmentation, and the "least privilege" approach can help abstract HVAs and provide access only to appropriate parties.

Organizations need to couple these innovations with partnerships to optimize and expand their current security architecture, not necessarily to add more technology. They should look to consulting firms to assist with the global road map of how to transform organizational strategy into architecture for the future. Organizations should design a measured, stair-stepped journey that brings their architecture to the doorstep of the evolving digital business — a security architecture that is agile, evolutionary, and flexible for the future. This architecture should be able to integrate all the industry-first and next steps of this digital age (e.g., use cases such as advanced robotics, autonomous vehicles, and remote surgery) and, most importantly, handle everything at the speed of digital business via hybrid, multicloud, multiedge, and 5G environments.

Organizations need to find partners to help the them sense and see more of the threat landscape through artificial intelligence and machine learning using automation and orchestration platforms to visualize, detect, and respond to threats. Ultimately, cybersecurity is evolving to design security by outcomes — intelligent outcomes.

About the Analyst

Christina Richmond, *Program Vice President, Security Services*

Core research coverage for Ms. Richmond's team includes, but is not limited to, security consulting, integration, and managed services. In addition, the team looks at services that help organizations adopt emerging technologies like cloud, edge, and IoT as well as key focus areas such as risk, data privacy, and compliance.

MESSAGE FROM THE SPONSOR

About Micro Focus

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges. The ultimate goal of cyber resiliency is to help an organization thrive in the face of adverse conditions (crisis, pandemic, financial volatility, etc.).

Micro Focus develops integrated cybersecurity solutions to enhance your intelligence and cyber resilience and protect against advanced cyberthreats at scale. To learn more about becoming cyber resilient, please take our 360-degree assessment at ***www.cyberresilient.com***.

IDC Custom Solutions

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.