IDC MARKET SPOTLIGHT

Sponsored by: Micro Focus

The goal of cyber-resilience is to ensure the enterprise's ability to withstand challenges and disruptions during strenuous times.

Are We Cyber-Resilient? The Key Question Every Organization Must Answer

November 2020

Written by: Craig Robinson, Program Director, Security Services

Introduction

Living through unprecedented times, enterprises have had to pivot and respond to the COVID-19 pandemic in ways they never expected.

Cybersecurity had traditionally been based on a linear, predictable, and somewhat static capability centered around waterfall change management, consistency, and predictability.

COVID-19 then shifted the paradigm. The C-suite shifted its focus almost overnight to resilient business operations and customer experience programs, which address activities critical to the viability of an organization in a time of crisis. Organizations had to adapt to unprecedented change to support business and organizational resilience, whether through adoption of customer outreach (channels), digital transformation (DX), artificial intelligence/automation, or conversion of supply chains.

The modern chief information security officer (CISO) similarly was compelled to support organizational resilience, address workforce changes, tackle enhanced insider threat concerns, protect an expanded risk surface due to the rush to the cloud, and deal with an explosion of targeted phishing attacks.

Senior leaders and boards of directors were forced to challenge their view of the organization's cybersecurity. If a major cyberattack were to hit the business, could they still perform their core mission during and after the attack? How resilient were their systems to a sustained campaign?

Questions surrounding resilience are not limited to cyberattacks from a nation-state or criminal syndicates. Insider threats have become more common as employees, contractors, or even third-party vendors with access to vital cloud-based company data are able to damage, delete, or exfiltrate these assets for their own financial gain. Are businesses resilient enough to withstand the intentional or accidental breach of regulated data such as employee social security numbers and work history?

AT A GLANCE

KEY STATS

According to an IDC survey conducted during the early stages of COVID-19, U.S. companies with 100–10,000 employees identified the following as their top 3 concerns when it comes to securing their business operations and IT environments: data breaches (55% of respondents), malware (52% of respondents), and targeted attacks (45% of respondents).

WHAT'S IMPORTANT

Having a culture of cyber-resilience that permeates the organization will allow new technologies such as 5G-enabled Internet of Things devices to be introduced in a safe and secure manner.

Warehouse distribution centers and manufacturing shop floors are increasingly reliant upon 5G-enabled robots and other automated machines to fulfill vital operations. Their tolerance is minimal for any sustained downtime due to cyberattacks or to outages in the edge computing devices or cloud fabric where so many business and industrial functions are performed. Boardroom discussions need to include asking how prepared department heads are for any major disruptions.

CISOs are used to being asked, "Are we secure?" After all, cybersecurity for most firms has seen a substantial funding increase in recent years. The new question that needs to be raised with CISOs, CIOs, chief manufacturing officers, chief medical officers, and other vital department heads is, "Are we cyber-resilient?"

What Is Cyber-Resilience?

IDC defines cyber-resilience as the merging of cybersecurity, risk management, business continuity, and resilience practices that further the organization's ability to withstand and recover from any accidental or deliberate attempt to keep the organization from performing its core functions.

An important distinction is that cyber-resilience does not have the same definition as cybersecurity. Yes, they share a common theme of preventing cyberattacks and keeping the business running. The key differentiator is that cyber-resilience widens the scope beyond cybersecurity to ensure an organization can absorb and withstand deliberate attacks, accidental breaches, or "acts of God." Cyber-resilience pays special attention to "what if" scenarios such as nation-state-sponsored cyberattacks against critical cyberinfrastructure and more accidental types of incidents such as a sustained email outage or disruptions to a key third-party supply chain partner.

How Is Cyber-Resilience Achieved?

It Is a Team Sport

Cyber-resilience is not the responsibility of the security team alone. It requires a multidisciplinary, organizational, and supply chain integration approach to support the transformation from cybersecurity to cyber-resilience. A select representation of the stakeholders in the development of cyber-resilience includes (but is not limited to):

- **The board.** Cyber-resilience will occur only when the leadership at the very top is engaged. The board is a perfect place to set expectations of cooperation between departments as well as to ensure that progress for various cyber-resilience projects remains on the agenda.
- **Outside stakeholders.** Cyber-resilience does not occur only within the walls of the enterprise. In today's digitally connected world, enterprises need to review the cyber-resilience of their supply chain. Is there language in the managed service agreements that supports cyber-resilience? Have alternative vendors been vetted to replace the primary vendor if there is a major disruption in that vendor's ability to service the enterprise?
- **Industry-specific C-suite**. Chief medical officers in healthcare, chief manufacturing officers in manufacturing, and chief supply chain officers will need to educate other team members about the critical items in their respective departments. The participation of all departments in various tabletop exercises and consultation on various "what if" planning sessions is also vital.

- **Legal, risk, and compliance officers.** Various governmental bodies are taking an increasing interest in the cyber-resilience of various industries deemed to be of national importance. Having legal, risk, and compliance officers in a position to address the changes that external bodies dictate is essential.
- **CISOs.** Cyber-resilience is not the same as cybersecurity, but it is fair to say that they both have a very significant part to play. CISOs need to be able to simultaneously lead, advise, and do the legwork on multiple projects related to cyber-resilience.
- **The bench.** When the starting players on a sports team get tired or injured, the head coach needs to be able to turn to the bench for help. Cyber-resilience teams need to have a bench to turn to for their own resilience. Cyberdisruptions do not occur on a timely schedule. When these disruptions occur when a "starting team" member is out, a prepared bench player must be ready to step in.

Steps to Becoming Cyber-Resilient

In today's interconnected business world, key business functions, or even entire departments, can quickly be outsourced. Cyber-resilience teams need to start thinking about the ramifications of rapid business changes and interdependencies while preparing for a breach or even functioning as if a breach has occurred.

The first step toward achieving cyber-resilience is aligning the cyber-resilience team with the organization's strategic direction. Prior to DX, strategic changes in enterprises were made over longer periods of time. Applications were built using a waterfall methodology of development with the timelines stretched over months or years. DX has caused a paradigm shift by shrinking development times to weeks, and the term AppSecDev is replacing AppDev in a nod to the additional role that security is playing in the new agile method of developing apps. Enterprises need to make sure that these new cloud-hosted apps are still properly aligned with the strategic business direction from the C-suite while ensuring that they have the resilience to survive disruptions from cyberattacks, hybrid cloud outages, or third-party supplier downtime.

The evolving presence of robots as a key component on the manufacturing shop floor is just one of the fascinating developments that the fourth industrial revolution has created. Interruptions to robot productivity due to malware or electrical power fluctuations can cost enormous amounts of money as production lines can halt if traditional cybersecurity actions are taken to forensically diagnose and remove malware in the robot. A properly aligned cyber-resilience team will have the operations, IT, and cybersecurity teams aligned and educated on the differences involved in removing malware from a multimillion-dollar robotic arm versus a $1,000 laptop used by a regional salesperson.

Consider the challenges of autonomous self-driving cars. They can't just stop moving their precious human cargo to their destination because of an outage in the 5G carrier's network. They need to have the self-healing capabilities that allow them to switch to a backup real-time mapping system, just like they need to have the capability of surviving a cyberattack while on the move.

The second key step in achieving cyber-resilience involves developing and following a proven plan or framework. This step is made easier thanks to proven frameworks that exist in the common domain. In November 2019, the U.S. National Institute of Standards and Technology (NIST) came out with a cyber-resilience engineering framework (NIST SP 800-160, Volume 2) that provides goals, objectives, and techniques. Like its sister framework on cybersecurity, the NIST cyber-resilience framework is a cross-disciplinary framework for cyber-resilience teams to follow.

Other publications provide cyber-resilience teams with guidance and frameworks to develop cyber-resilience plans for their organizations. The Software Engineering Institute has published the CERT Resilience Management Model, which is a full-featured cyber-resilience framework. Longtime cybersecurity professionals will find a familiar name and model in the MITRE Cyber Resiliency Engineering Framework. For example, its mapping of cyber-resilience techniques to actual objectives has the same feel as that of the MITRE ATT&CK framework.

The third step in achieving cyber-resilience is recognizing what is at risk and identifying potential or likely adversaries. This step is a combination of identifying the actual assets that need protection and mapping out the various locations where they can be found. Some of the more nontechnical team members really come to prominence at this point.

HR departments will recognize the importance of keeping employee data secure. Manufacturing or research personnel will recognize the value of keeping intellectual property (IP) from being exfiltrated. Healthcare and medical insurance providers will recognize the value and regulatory importance of protecting personal health information (PHI).

It is important for the cyber-resilience team to account for an asset even if it is directly or indirectly controlled by a business partner. Time and attention will need to be paid to third-party enterprises. Their continued relationship with your organization should include securing a regular risk score from a reputable firm. The score should reflect the partner's cyber-resilience and the amount of risk faced by assets under the partner's control.

A robust threat intelligence program is the best way to determine which entities have the capability and desire to inflict harm on the enterprise. This is where a layered defense portfolio that subscribes to multiple threat intelligence feeds comes in handy. It can help identify all of the potential threat actors as well as their tactics and procedures and provide a horizontal view of the threat actors in the region(s) and industry.

Step four in pursuit of cyber-resilience is to instill the mindset that this is a team game. Remember, cyber-resilience is not the exclusive domain of the cybersecurity team. CISOs need to be leaders, coaches, change agents, and cyber-resilience evangelists. Sometimes, the security team needs to take a seat on the bench and support its marketing and IT teammates as they seek to make marketing assets cyber-resilient. At other times, the security team will partner internally with supply chain professionals as they validate whether partners in their supply chain are susceptible to cyberdisruptions that could impede their ability to fulfill key contracts.

The board needs to continue its oversight and participation in cyber-resilience efforts. Making cyber-resilience projects a regular review item will help ensure the resilience of both individual interconnected systems and the whole organization.

Cyber-Resilience Goals

One of the goals of cyber-resilience is to ensure the enterprise's ability to withstand challenges and disruptions during strenuous times. Achieving this objective will help secure the continued existence of the enterprise.

One of the more recently updated frameworks around cyber-resilience comes from NIST, which laid out its four key goals to achieve cyber-resilience:

- **Anticipating disruptions.** A robust cyber-resilience program involves detecting attacks that a cybercriminal might be launching at a firm. This component is largely a recognition that protection will not always work. Attacks will land. A strong cyber-resilience program can utilize artificial intelligence and machine learning to correlate device and business data to anticipate and triage attacks, recognize the true threats from threats of lesser importance, and automate the response functions to get system(s) back to predisruption performance levels.

- **Withstanding disruptions or attacks on key systems.** This is where layers of defense can be crucial. Has the CIO set up cloud services to ensure that an outage at any one cloud hosting facility would trigger a redundant cloud facility to automatically take over? Has the chief supply chain officer worked with the CISO to identify suitable cyber-resilient companies that could supply crucial components need on the manufacturing shop floor?
- **Recovering from sustained attacks or disruptions.** Having a strong incident response program is critical to attack response. Organizations should practice a response plan ahead of time that prioritizes the steps needed to recover key systems. Key elements should include:
    - Tabletop exercises so that everyone knows their roles and responsibilities in case the incident response team is deployed
    - A well-thought-out and communicated incident plan and playbook to provide the structure that will be put into place in the event of an incident
    - Engaging red (simulated attack) and blue (defense) teams to simulate and measure how well the organization defends itself
    - Technical playbooks that allow for automated response
- **Adapting and modifying the organization's capabilities to address potential threats.** The importance of having a robust strategic threat intelligence program cannot be overstated. Incorporating multiple feeds with contextual intelligence that identifies who might be targeting a firm's industry or region or the firm directly is beneficial.

Trust and communication between the board and the CISO now become crucial. Understanding the organization's strategic and tactical direction allows the CISO to direct threat intelligence teams to look for potential adversaries.

Utilizing this intelligence can help a firm and its security team prioritize what systems need to be patched or modified based on potential threats. When the inevitable attacks do find a landing spot, a good threat intelligence service can forensically identify the likely strategies that a cybercriminal might be employing.

Some nation-state actors will try and "live off the land" and exfiltrate valuable data. Other cybercriminals will specifically seek to launch ransomware attacks as quickly as they can, while still others will seek to destroy and plunder as much as possible. Regardless of tactics, a key to achieving and maintaining cyber-resilience is rapidly detecting threats that make their way into an organization's environment. Utilizing the previously mentioned playbooks and other automation technologies will pay big dividends in reducing the dwell time that attackers can persist in the environment.

Achieving these four goals will set up an organization with a solid foundation for cyber-resilience, but the ultimate benefits will be the recognition and the confidence that the firm is much more likely to survive any major cyberincident that comes its way.

Considerations

Cyber-resilience is a paradigm shift to enable enterprise resilience and the ability for organizations to thrive despite adversaries, crises, and business volatility. Being resilient will equip organizations with the ability to "pivot" at scale during adverse market conditions (including nonbusiness events such as a global pandemic) and adapt to customer changes, digital transformation, and hyperscaled growth.

The business case for cyber-resilience can and should measure the savings that could be achieved by having a system in place that mitigates the potential loss to the ability of an enterprise to perform its core mission due to a cyberevent. Potential cyber-resilience investments must always take into account the amount of risk that is mitigated due to the inclusion of the particular measure being implemented.

Conclusion

Board members are adding the topic of cyber-resilience to the agenda for the foreseeable future to ensure that CISOs and the C-suite are fully engaged with each other on this important function. Important cyber-resilience discussions need to rise to the very top of the organization.

Setting up a strategic and robust cyber-resilience program requires an "over the horizon" type of vision. Organizations that think that just having a good cybersecurity program is enough to make them cyber-resilient will not fare well. A strong cyber-resilience program gives an organization a much more holistic view of all of the key systems and processes that are in place.

The new question that needs to be raised to CISOs, CIOs, chief manufacturing officers, chief medical officers, and other vital department heads is, "Are we cyber-resilient?"

When the inevitable cyberdisruption occurs, stakeholders will be thankful that there is a well-thought-out and practiced cyber-resilience plan in place to help ensure the organization can survive and thrive during turbulent times.

About the Analyst

Craig Robinson, *Program Director, Security Services*

Craig Robinson is a Program Director within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include IoT security, blockchain services, and threat detection and response services. Mr. Robinson delivers unparalleled insight and analysis, leveraging his unique experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

MESSAGE FROM THE SPONSOR

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 ***cyberresilient.com***.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on **www.idc.com**.

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