DXC.technology

DXC Labs | Security

Build cyber resiliency into the enterprise

Strategies for adapting systems and evolving cultures to meet rapidly changing threats

The fact that your organization will be compromised is a given in today's hyperconnected world. As organizations put more stock into digital efforts, rely more heavily on technology such as cloud, and shift toward remote working, attackers are becoming more sophisticated, more resourceful and better organized. The collision course is unavoidable.

Cyber resiliency enables organizations to survive attacks, maintain operations and continue to execute their strategy in the face of evolving threats.

The goal, then, is not just to prevent attacks, but to be able to survive them and maintain operations — to become cyber resilient. Cyber resiliency should be part of a holistic approach to security that takes all aspects of the business into consideration, from employees and partners to the board of directors. Improving security is not a one-time project, but a program of continuous improvement focusing on optimized outcomes.

The U.S. National Institute of Standards and Technology (NIST) defines cyber resiliency as "the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources."[1] More realistically, cyber resiliency is also about establishing a policy and process that help an organization to survive and continue to execute its long-term strategy in the face of evolving security threats.

To become cyber resilient, enterprises must strike a balance between protecting critical assets, detecting compromises and responding to incidents. Making the IT landscape cyber resilient requires investments in areas such as infrastructure, design, and development of systems, applications and networks. At the same time, organizations must create and foster a resilience-conscious culture, of which security is an essential part.

This white paper details the strategies, steps and considerations needed to establish cyber resiliency while enabling your organization to adapt systems and evolve cultures as the threat landscape changes.

The evolving threat landscape

By many measures, the number and intensity of cyberattacks continue to rise, as nimble adversaries become more sophisticated and find new ways to target enterprises. In the race to adopt digital capabilities, businesses open their employees, customers, applications, devices and data to increased access from internal and external threats.

Today's cybercriminals are often well funded, some even sponsored by rogue governments. Stealthy and persistent attackers now have the skills and tools to do everything from taking down power grids to targeting hospitals and financial institutions with ransomware. The new breed of cyberattack can employ advanced persistent threats (APTs) and might include techniques such as remote-controlled malware to disrupt systems. The consequences can range from enormous financial losses to severe reputational damage.

Attackers with next-generation threat capabilities are transforming faster than most organizations can keep up. Their common goals are becoming increasingly aligned, and malicious code shows signs of reuse and collaboration.

As if that weren't enough to deal with, regulatory pressures are causing an increase in security costs and complexity, with the 2018 implementation of the European Union's General Data Protection Regulation (GDPR) serving as a prime example. The California Consumer Privacy Act of 2018 also enables insights into the U.S. state-level regulatory patchwork that is on the horizon.

Add everything up and it isn't surprising that the global economic impact of cybercrime is growing. A November 2020 report conducted by Cybersecurity Ventures predicts that the annual cost of cybercrime worldwide will reach $10.5 trillion by 2025.[2] Each data breach will cost organizations an average of $3.86 million, according to a report prepared by Ponemon Institute.[3]

Take the right route to cyber resiliency

Escalating threats make it clear that, regardless of what you do, you cannot protect against everything. All organizations need to plan for allowable levels of vulnerability based on their risk tolerance. Instead of solving a specific problem, enterprises must establish built-in resilience that allows them to adapt, evolve and change their security posture.

To foster resiliency, you must design for it, with a focus on protection, detection and response. And because attack details change, strategies should seek to address general principles and classes of threats, not technical details of the threat du jour. An enterprise cyber resilience strategy includes three main components.

1. Adapt existing business and IT systems to next-generation threats.

Cyberattacks primarily come in three forms. The first is global malware and ransomware attacks. The second is much subtler, where the adversary lurks inside the network, gaining access to resources and information as needed. The last is the hardest to defend — an insider attack by a rogue staff member with knowledge of the environment. Prepare for all types of attacks by addressing issues at multiple levels.

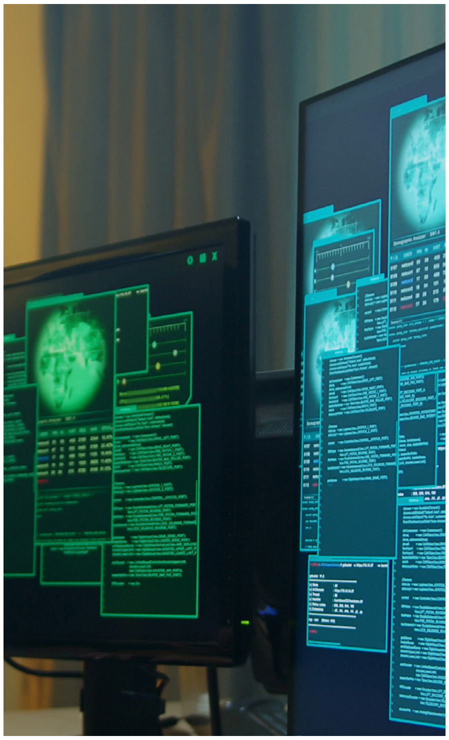
Think strategically with assessments and plans. Begin by defining your enterprise security architecture to address prioritized risks. Get a fresh baseline of your current security stance by asking questions that would not have been asked even a few years ago. For example, find out how your enterprise would recover from ransomware if multiple sites, the Active Directory and backup platforms became encrypted.

Evaluate critical applications and their dependencies on infrastructure and core capabilities, such as directory and network routing, identity and access management capabilities, and endpoint access. Assess platform and product risks, and adjust policies and governance as needed.

Define a communications and command structure to ensure business continuity. Previous business continuity plans were not designed for a full platform-level infection, and even crisis management is different when there is no email, online conferencing or internet access. Include coordination actions for partners and suppliers who must act effectively in response situations.

Operate optimally using a holistic approach. Coordinate and orchestrate security monitoring and breach responses at an operational level to optimize defense, response and recovery for networks that are segmented with simplified directories and that control top-level access.

Configuration management databases (CMDBs) are critical to understanding the deployment and interdependencies of enterprise applications. Organizations can't adequately defend against attacks if they don't know where their key assets reside. Therefore, ensuring high data quality of the CMDB can mean the difference between an uneconomically recoverable incident and a readily actionable response plan that can be automated through orchestration and ticketing. Take a holistic approach to operational security with critical end-to-end visibility and proven processes that grant security managers and other key personnel the authority to act independently when decision speed is imperative. Consider, however, that many parts of your organization may be managed by third parties or partners. These individuals and entities also require empowerment to isolate systems when there is significant risk.



Take a technical snapshot before planning and rebuilding. Conduct a full inventory of all assets and capture key interconnections for a detailed picture of your infrastructure. Use it for planning and as a rebuild target when recovering.

Document clear security policies for storing workloads on platforms, which is where most attacks occur.

Create platform-specific compartments that isolate and segment network traffic — especially when using older versions of products. Implement current password management and access control tools inside the perimeter to prevent credential stealing. Architect networks with appropriate network segmentation controls, software-defined networking, flow-based rule sets, hierarchical network design and microsegmentation based on the risk of the data being processed. Also use intra- and intercompartmental encryption, plus traditional firewalling between network segments.

2. Update your cybersecurity governance strategy.

As noted, attackers are either after your data to monetize it or want to disrupt your business by disabling your infrastructure. Although you can't completely secure everything in the enterprise, by strategically focusing on critical digital assets and the interactions between them, you can proactively protect your data and applications and control access to both, regardless of user location or device.

Governance is essential to successful security planning and key to attaining cyber resiliency. To ensure that your strategy measures up, incorporate policies for protection, detection and response.

Protect critical assets through proactive planning. Update and test business continuity and crisis management plans to cover new models of sourcing. Expand crisis management requirements to include all partners and suppliers. Make board members aware of cyber risks and the steps to effective cyber resiliency.

Review and refine older access and software-patching policies so they align with next-generation governance strategies. For example, determine whether to adopt therecommendations of NIST and other national security organizations, which emphasize password complexity rather than frequency of change.

Consider adopting role-based access control (RBAC) to more efficiently regulate access to computer and network resources. For example, system administrators are likely to require more complex passwords or multifactor authentication than general users. RBAC simplifies this process because it doesn't use access control lists (ACLs), which require translating people to a group or organization.

Detect next-generation threats with enterprise-wide visibility. To enhance detection, increase monitoring of behaviors and identities when a suspected compromise is underway.

Gain enterprise-wide visibility by implementing security controls across data, users, networks and endpoints. Tier cyber defense platforms and integrate solutions and services using a variety of models — such as software as a service (SaaS), hybrid or customized solutions — to identify abnormal patterns frequently found in user and application layers, where advanced attackers create long-term back doors and patiently seek key information.

Changing the corporate culture is rarely easy, especially when it involves adjusting how personnel perform familiar tasks. But to achieve cyber resiliency, it's important to go beyond establishing a security-conscious culture to fostering a resilient one.

Respond rapidly to preserve business continuity. Define a clear incident response strategy that spells out lines of authority and responsibilities during an incident and captures all procedures and best practices for the response. Most companies lack the skilled personnel and capabilities to adequately respond to a major attack or breach, and unfortunately, most wait until after the incident to seek outside assistance. Time is of the essence with regulatory mandates, such as the European Union's GDPR requiring companies to report data breaches within 72 hours. That's why it's crucial for companies to retain third-party incident response services. Security teams can work together to understand the environment and the security architecture before a catastrophic attack happens. It could mean the difference between having incident response experts on the job within hours of detection — or waiting days or even weeks to hire a new vendor.

During the recovery phase, identify a location for overseeing recovery efforts when geographically feasible. Identify the complexity of the compromise. If an application has been exploited, removal is simple. However, a compromise of an operating system or kernel will require rebuilding the standard operating environment with a suite of tools that should include antivirus, host-based intrusion detection systems, and endpoint detection and response. In the case of a hardware or root kit compromise of the device, physical replacement may be required. The critical success factor is to have applications hosted on standard operating environments and a well-documented or automated configuration process to ease their redeployment.

3. Create a resilience-conscious culture.

Changing the corporate culture is rarely easy, especially when it involves adjusting how personnel perform familiar tasks. But to optimize outcomes in the event of an attack, it's important to go beyond establishing a security-conscious culture to fostering a resilient one.

Think beyond security. Design for good security and resilience, not absolute security. For example, the most secure systems are not necessarily resilient. One person may only understand a system locked away in a strong room. Achieve business continuity by replicating best practices and identifying multiple administrators.

Educate the first line of defense. Encourage all employees — not just the cybersecurity team — to adopt a cyber resilient mindset. Stress that employees are the first line of defense when it comes to threats such as phishing and malware. Explain the importance of being fully conscious of the consequences of a security breach. Build continuous employee education and practices into your security plans.

Managers should be particularly aware of their values, actions and decisions, which have a twofold impact — affecting the security of their own data and systems as well as modeling proper cyber resilience practices for employees. To increase awareness and turn a critical eye on themselves, managers should make use of established frameworks such as those used in the safety industry to assess human and organizational risk factors.

To increase awareness and turn a critical eye on themselves, managers should make use of established frameworks such as those used in the safety industry to assess human and organizational risk factors.

Foster collaboration across the organization. Promote collaboration across teams with pertinent information about security and threats. Coach employees to share knowledge with appropriate authorities and peers both within and outside the enterprise. Hold staff accountable for fostering a resilience-conscious culture through collaboration.

Accelerate the drive to resiliency by constantly looking ahead

The world continues to rapidly change as next-generation threats move in. Study the impact of today's trends and adjust your organization's security strategy before trends turn into issues that slow the journey to cyber resiliency.

Adapt security management for a perimeter-less world. Before COVID-19, organizations were already embracing digital transformation and migrating data and workloads to cloud. The coronavirus accelerated the adoption of cloud and other technologies necessary to enable remote work and allow staff to access data from any location.

This shift has moved the emphasis away from protecting infrastructure and on-premises data with traditional network security measures such as firewalls, proxy servers and VPNs. With less infrastructure to manage and protect, and with data breaches on the rise, the focus is now on protecting data, regardless of where it is hosted and how it is accessed.

To mitigate the security impact of this shift to remote access, organizations are beginning to embrace zero-trust architecture, a model that assumes everything around a network is hostile, including network assets from the trusted zone. All access to the network assets is, by default, not trusted, and thus is continuously validated. Access is kept to a minimum and permitted only based on certain policies and within the right situational context.[4]

Prepare for internet of things (IoT) vulnerabilities. Consider the system's cyber and physical security requirements and resilience before widely deploying and depending on IoT systems. Hackers often use enterprise devices as backdoors into systems with troves of sensitive data, making them unsuspecting agents in distributed denial-of-service (DDoS) attacks.

Ensure that hardware-backed, device-unique security credentials are keyed and changed according to best-practice cryptographic standards to reduce the attack surface and limit compromise to individual devices. Use IoT gateways and edge devices to segregate and provide layers of protection between insecure devices and the internet to help manage the overall lack of IoT security.[5]

Rely on resources in security operations centers (SOCs). Examine the important role SOCs play in bringing together the resources needed to direct the defense of digital and physical assets and in enabling key business initiatives. SOCs:

- Define what constitutes suspicious activity, identify vulnerabilities, configure detection technologies, search for and validate active threats and ultimately notify affected parties
- Manage and monitor identities for users, machines and applications
- Leverage automation and orchestration capabilities to accelerate common monitoring and response activities
- Ensure compliance with internal policies and government regulations

Consider deploying one or more SOCs using in-house resources, or outsource your SOC to a specialized security team.[6]

Adopt a DevSecOps approach to digital transformation. To bolster cyber resilience, consider adopting a comprehensive DevSecOps model that incorporates review and governance and supports faster release schedules and innovation.

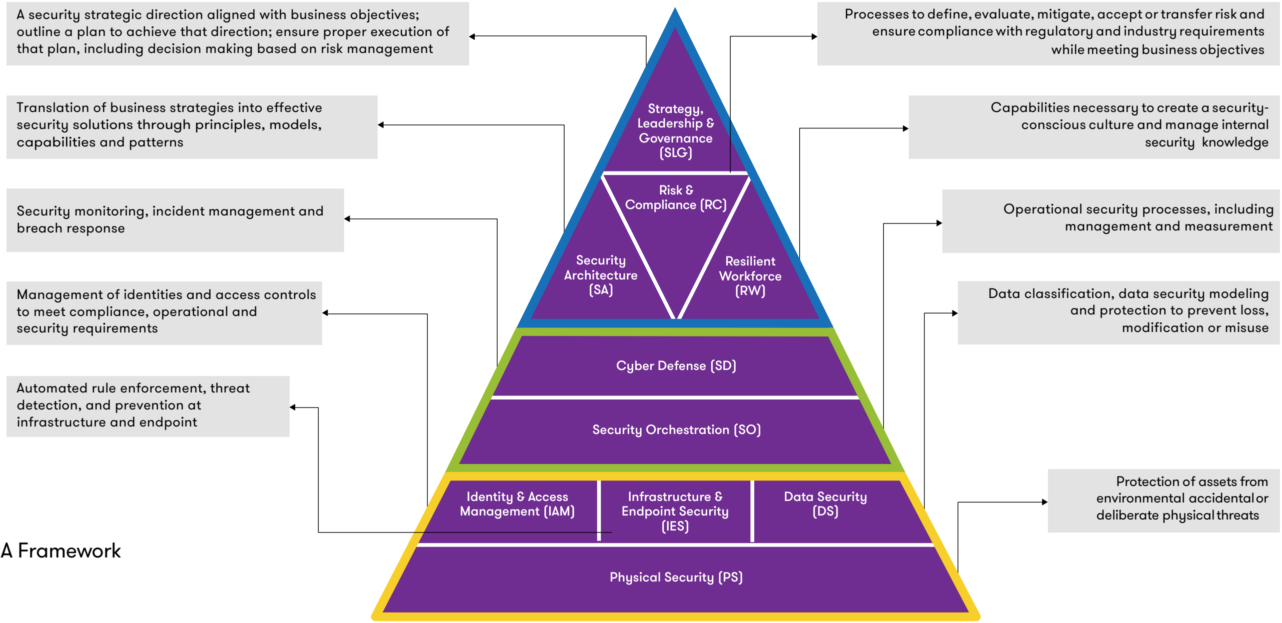
Determine whether your organization can commit to requirements necessary for success, which include changing to a culture of collaboration, building security throughout the development life cycle, and evaluating technical and business risks.

Examine the practice of abstraction, in which developers push technology risk to a layer, such as the cloud, where it becomes invisible and forgotten. Incorporate the practice into your security plan as appropriate. If not, know that by taking a DevSecOps approach to digital transformation, you can still apply security policies and procedures at each stage of the development process.[7]

Avoid costly delays with a better reference architecture

Achieving cyber resiliency involves putting all the pieces of a security strategy into place, including technology, governance and cyber defense platforms — all backed by an effective reference architecture. Leveraging best practices learned from deploying hundreds of engagements for many of the world's largest organizations, DXC Technology has developed a comprehensive Cyber Reference Architecture (CRA), shown in **Figure 1**, CRA Framework. It serves as the foundation upon which we design and deliver security solutions that optimize security spending and improve operational effectiveness.

The CRA presents a highly structured way of thinking about enterprise security. It ensures that all areas of IT security are taken into consideration for resilience. The framework is technology independent, and like any good IT security strategy, it is closely aligned with relevant industry standards and best practices. The CRA advocates a proactive and integrated approach to cybersecurity that starts with a clear understanding of risk across the organization, with a focus on critical assets and interactions to manage risk and security throughout the enterprise.


Strategy, Leadership & Governance (SLG)
Risk & Compliance (RC)
Security Architecture (SA)
Resilient Workforce (RW)
Cyber Defense (SD)
Security Orchestration (SO)
Identity & Access Management (IAM)
Infrastructure & Endpoint Security (IES)
Data Security (DS)
Physical Security (PS)

A security strategic direction aligned with business objectives; outline a plan to achieve that direction; ensure proper execution of that plan, including decision making based on risk management

Translation of business strategies into effective security solutions through principles, models, capabilities and patterns

Security monitoring, incident management and breach response

Management of identities and access controls to meet compliance, operational and security requirements

Automated rule enforcement, threat detection, and prevention at infrastructure and endpoint

Processes to define, evaluate, mitigate, accept or transfer risk and ensure compliance with regulatory and industry requirements while meeting business objectives

Capabilities necessary to create a security-conscious culture and manage internal security knowledge

Operational security processes, including management and measurement

Data classification, data security modeling and protection to prevent loss, modification or misuse

Protection of assets from environmental accidental or deliberate physical threats

Figure 1. CRA Framework

Work securely with everything you need to achieve cyber resiliency

Cyber resiliency needs to be a top priority for any organization — from the board of directors to every employee. There needs to be a sense of urgency, coupled with the agility to adapt and respond quickly. Whereas a natural disaster or random failure may affect just one part of a company, an intelligent attacker can pose a risk to all systems around the globe at the same time. Thus, IT security should be planned with a holistic approach that considers all aspects of conventional business continuity while also taking into account the goals and aspirations of the attacker.

Achieving cyber resiliency should be a modular transformation that evolves from a well-defined strategy to a project roadmap. Begin by defining a security strategic direction aligned with your business objectives, outline a plan to achieve that direction and ensure proper execution of that plan, including decision making based on risk management. A list of initiatives can be scoped out after thorough risk and cyber maturity assessments.

Cyber resiliency is an ongoing pursuit. To succeed, your organization must:

- Develop a clear, holistic strategy
- Establish clear governance
- Change the way people view security
- Embrace emerging technologies and trends
- Back up your plan with a rock-solid reference architecture

A measure of cyber resiliency can be accomplished by mapping all objectives to deliverables to ensure the full traceability of benefits. At the same time, enterprises need to be continuously monitoring and adapting, because the bad guys will never rest and will always be coming up with new ways to attack. While you can't keep the bad guys out forever, your cyber resistant culture can minimize the distraction and damage while ensuring that your organization stays focused on the business at hand.

Contributors

Rhodri Davies, security architect for Security Cyber Defense, DXC Technology

Gary Roberts, security enablement for Security, DXC Technology

Richard McEvoy, senior risk advisor for DXC IT, DXC Technology

Alex Kreychman, cyber security engineer for Security in the Americas, DXC Technology

TM Ching, chief technology officer, Security, DXC Technology

References

[1] NIST: Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, March 2018

[2] Cybersecurity Ventures, 2021 Report: Cyberwarfare in the C-Suite, November 2020

[3] Ponemon Institute , The Cost of Data Breach Report 2020, July 2020

[4] DXC White Paper: Zero Trust for maximum security, May 2020

[5] DXC White Paper: 10 steps to securing the internet of things, April 2018

[6] DXC Technical Deep Dive: Putting on the right SOC to fit your security operations, April 2018

[7] DXC White Paper: Take a risk-based approach to DevSecOps, March 2018

DXC Labs | Security

DXC Labs delivers thought leadership and technology prototypes to enable enterprises to thrive in the digital age.

DXC Labs | Security brings together our world-class advisors to develop strategic and architectural insights to reduce digital risk. DXC's Cyber Reference Architecture is at the heart of our research, providing clients with detailed guidance on methods to efficiently resolve the most challenging security problems. We help clients minimize risk while taking maximum advantage of the digital commons.

Learn more at **www.dxc.technology/securitylabs**

Learn more at www.dxc.technology/ security

Get the insights that matter.
www.dxc.technology/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to provide services across the Enterprise Technology Stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.