Make your organization more resilient to cyber attacks

By Mark Hughes, DXC Technology

Companies must become cyber-resilient — capable of surviving attacks, maintaining operations, and embracing new technologies in the face of evolving threats.

The year 2020 will be remembered for many things. In cybersecurity circles, it was the year of the data breach.

While COVID-19 spread around the world and tens of millions of people moved to remote working, hackers and nation-state actors became more opportunistic, more sophisticated, and better organized.

Amid these converging forces, it's no longer a question of if but when your organization will experience a security breach.

A cultural shift

As we help our customers address this evolving threat landscape, I see more companies realizing that security is not just a technology issue. It's a problem for the business and even the board of directors. Cybercrime will cost businesses $10.5 trillion globally annually by 2025, according to Cybersecurity Ventures — impacting brand reputation, customer confidence, regulatory compliance, and operations.

Simply being security-conscious is no longer enough, nor is having a prevention-only strategy. Companies must become cyber-resilient — capable of surviving attacks, maintaining operations, and embracing new technologies in the face of evolving threats. This means establishing policies and processes that strike a balance between protecting critical assets, detecting compromises, and responding to incidents.

Develop a clear, holistic strategy

Resiliency doesn't mean you can defend against all attacks; it means that if you are compromised, you have a plan in place that lets you recover quickly after a breach and continue to function.

Every company should define what resiliency means to them based on their business objectives, priorities, and risk tolerances for various systems and business areas. Instead of solving a specific problem, enterprises have to establish built-in resiliency that allows them to adapt, evolve, and change their security posture.

Before you can protect information assets, you have to know what they are and where they reside. Resiliency requires companies to conduct a technology inventory, identify critical application dependencies and vulnerabilities, and incorporate this information into recovery plans and rebuild targets. Knowing your infrastructure can help ensure a readily actionable response plan that makes an incident economically recoverable.

> Resiliency doesn't mean you can defend against all attacks; it means that if you are compromised, you have a plan in place that lets you recover quickly after a breach and continue to function.

The next step is to put in place and rehearse an incident response plan. Define a communications and command structure to ensure business continuity, with provisions for such contingencies as a ransomware attack that affects multiple sites or the need to conduct crisis management without internet access.

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 control access regardless of the locations of your employees or the devices they use.

Establish clear governance

A good incident response plan will clearly define who's responsible for which actions during an incident and will capture all procedures and best practices for the response. Without clear responsibilities, you may have a plan that nobody knows how to follow.

Your incident response strategy should enable you to escalate and respond rapidly, because time is of the essence to ensure business continuity and comply with regulatory mandates. That means ensuring your senior management and your board are aware of the strategy, as well as enlisting necessary third parties in advance, including partners, legal teams, incident-response services, and law enforcement.

Create a cyber-resilient culture

Resiliency can't be achieved just by creating processes and controls. What makes an organization resilient is the people in charge of the assets and data.

Every employee from the business staff to IT personnel to executives should adopt a cyber-resilient mindset, which begins with recognizing that they are the first line of defense against threats. Reinforce the culture with continuous security-awareness training—use gamification to let people experience the impacts of security policies, and reward them for doing the right thing rather than punish them for mistakes.

Embrace a Zero Trust mindset

Threats evolve quickly, and the security industry is always playing catch-up.

As security controls get better, adversaries become more creative with new strategies for attacks. One fact that has dramatically impacted security policies is that the security perimeter has become much more fluid and harder to manage. With more data in the cloud and in off-site data centers, and more employees working from

home using their own devices, security is no longer a matter of just protecting the trusted internal network zone.

Don't assume that your organization's prior investments in security controls will keep you safe. Keep up with the latest attack methods, and continually evaluate the relevance of your existing controls and plans.

To mitigate the security impact of this shift to remote access, organizations are increasingly embracing a Zero Trust architecture, a model that assumes everything around a network is hostile. Zero Trust requires continual verification and permits access based only on certain policies and within the right context.

Resiliency is a journey

Cyber resiliency begins with a well-defined strategy aligned with a project roadmap and lines of accountability. These plans ensure proper execution of the strategy with decision making based on risk management.

As a foundation, organizations should also have a solid cybersecurity architecture that provides guidelines to make sure the right infrastructure and controls are in place while allowing flexibility for technological change.

While no plan is 100 percent attack-proof, your cyber-resilient culture can minimize distraction, risk, and damage while ensuring that your organization stays focused on its mission-critical strategies.

Learn how to strengthen your security program. Subscribe to **DXC's Security Threat Intelligence Report**.

About the author

Mark Hughes is senior vice president of offerings and strategic partners at DXC Technology and is responsible for DXC's global security organization and offerings, including cyber defense, secured infrastructure, digital identity, and data protection. He previously served as chief executive at BT Security.