Leader’s Guide

BREAKING THROUGH WITH MODERN SECURITY:

How CIOs Can Enhance Cyber Resilience

One of the biggest priorities for CIOs right now is cybersecurity.

The recent rapid acceleration of digital transformation and distributed work has changed the game in cybersecurity.

When most employees worked exclusively from an office, the boundaries for cybersecurity were clearer. With do-from-anywhere work, the threat surface expands to wherever your employees go.

In the Dell Technologies Breakthrough study, (based on research with 10,500 people from 40+ locations),

72% of respondents said that the changing working world has exposed their organization to greater cybersecurity risk.

The challenge CIOs face lies in the intersection of effective cybersecurity measures and the realities of life. Nearly two-thirds of respondents (62%) said their employees are the weakest link in their security landscape. And the employees validate this concern, with more than half (56%) saying they have not substantially altered their security awareness or behavior, even with increased awareness of the risks.

This is a universal and human problem—even the most security-minded person is still prone to slip-ups. The most effective strategy isn’t to browbeat employees to adhere to existing, and potentially outdated protocols but rather to make sure your security posture accounts for the human factor.

As a CIO, you are responsible for securing seemingly infinite insecure locations. While your employees can provide some help, relying on their participation alone will not suffice. This responsibility can seem daunting, but it can be done.

Here’s what you need to know to keep your employees and IT infrastructure secure.

Top 5 reasons why respondents think their people fall victim to cyberattacks:

1. Overconfidence in the organization’s firewalls to stop threats
2. Not grasping the scale of the threat
3. Hopeful they won’t be targeted
4. Assuming the fallout can be easily resolved
5. Ignoring the threat because they don’t know how to resolve it

> “Security is everyone’s responsibility. With the rising security threat, businesses need to arm their employees with the right knowledge and an understanding they can help thwart cybercriminals if they follow the security requirements their organization has put in place. Businesses must also make that behavior the default through the deployment of intrinsically secure technologies and technology processes. Permeating the shared security responsibility message into the culture is paramount. Generally, people need to hear a message several times, in different ways, before it trickles down to behavior.”
>
> **John Scimone, Senior Vice President and Chief Security Officer, Dell Technologies**

Compensating for insecure behavior

CIOs and CISOs are responsible for deploying technology to secure the company’s digital assets. But what happens when the most insecure (and volatile) parts of the system are the people who use it?

Even with the best of intentions, human error is unavoidable. That’s why it’s important to have a plan for when—not if—your cybersecurity measures are put through the ultimate test of a real-world cybersecurity attack. This plan requires a responsive and scalable solution that achieves the following:

1. **Protecting data and systems:** Your solution should protect employees wherever they are working, and on whatever device they choose to work.
2. **Enhancing your cyber resilience:** Layers of security and disaster recovery capabilities are essential components.
3. **Overcoming security complexity:** A streamlined, easy-to-use solution will help increase compliance.

As CIO, it is up to you to fortify your business technologies and build trust with those that depend on them. To do this, you will need to answer some important questions:

- Does your organization’s cybersecurity cover the end-to-end IT ecosystem, including devices, applications and systems?
- How are you compensating for insecure end-user behavior? For instance, are you using AI-based optimization software to automate privacy controls when the user steps away from their device?
- Has your organization assessed the new and potentially greater risks posed by increased remote work?

Protecting data and systems

The complexity and silos inherent in a distributed workforce multiply the vulnerability to cyberattacks. Any time proprietary data is sent across clouds and remote work environments, that data is at risk.

These vulnerabilities can be offset with an end-to-end security model that overcomes silos and complexity, such as Zero Trust.

Zero Trust is an IT security model that is based on the notion that no interaction should be trusted and therefore every interaction should be verified. This authenticate-every-step model can be applied across your organization's network, IT infrastructure, software and microservices.

With a multi-layered, Zero Trust approach, a perimeter is created around every interaction. Even if a threat actor crosses one perimeter, they won't be able to exploit a presumption of trust based on their current access to the system. Each gateway they attempt to pass through requires authentication. These "deny-by-default" security protocols can help protect your data, your employees' trust and your trusted relationships with your customers.

Q As you begin fortifying your organization's systems to protect applications and data, consider these key questions:

- Is your overall security posture moving towards a Zero Trust model?
- Do your vendors and internal DevOps team have appropriate cybersecurity measures in place to ensure a secure development lifecycle that protects the processes by which new products, features and services are developed/implemented?
- Is your current security capability bolted on or built in? Siloed or unified? Threat-centric or context-centric?

Preserving your data is where and how your backup data is stored. Before compromising your core data, cyberattackers will typically attempt to compromise your backups.

Enhancing cyber resilience

As the saying goes, **"The only thing harder than planning for a disaster is explaining why you did not."**

At the crux of achieving cyber resiliency is assuming an attack will occur and taking prospective steps to recover as quickly as possible, with minimal financial and operational impact.

Those steps include conducting simulations that stress test your business and operational continuity and recovery systems, as well as your cybersecurity response and corporate response across key functions like legal, crisis management and communications.

However, this sort of rigorous testing can be time consuming. A managed solution can take these tasks off your team's plate and will stay on top of emerging threats and trends in cyberattacks. For instance, a managed threat detection and response service will sift for threats and probe your company's responses for you.

Another important consideration is preserving your data, which means knowing where and how your backup data is stored. Before compromising your core data, cyber attackers will typically attempt to compromise your backups.

The best defense against this is an isolated, offline copy of your critical systems. The story of Founders Federal Credit Union (FFCU) provides a useful illustration of how and why this can be done.

FFCU calculated that, should a cyberattack such as ransomware happen, they had a one-hour window in which to recover their data and resume operations. This led them to conduct a major overhaul of their data center's cybersecurity with a focus on getting back up and running quickly. They implemented a cyber recovery vault, which sits behind an operational "air gap" that keeps it separate from their system while still regularly syncing production data. This lets FFCU be confident that their data will always be available, protected and uncorrupted.

Q As you look to bolster your cyber resilience in an evolving security landscape, consider these questions:

- Has your organization determined the amount of time its operations would be disrupted in the event of a cyberattack?
  - If so, is it minutes, days or weeks?
- When was the last time you identified business-critical workloads and data to put in isolated protection?
- What type of threat detection capabilities do you have in place?
  - Is this managed internally or by a third party?
  - Does your organization use AI-based pattern anomaly detection?

Complexity is the enemy of security

When your security operations team is managing solutions for your wide array of IT infrastructure components, the complexity, and therefore risk, can mount quickly. With this complexity also comes increased cost and inefficiency in your regular operations. Finding a balance between these usually results in unsustainable compromise on both fronts.

There is a better way to scale your cybersecurity operation. You can free up time and resources with advanced security tools that use artificial intelligence (AI) and machine learning (ML) to enable more consistent governance and behavior.

AI tools help your threat detection solutions identify and report anomalies in the network, as well as policy violations, which would initiate a cascade of security actions. Automated security can also improve software development code. With fewer mistakes and human errors, comes fewer vulnerabilities.

However, to unlock maximum value from your security tools, you need them to be easy to use and manage. By consolidating your organization's security applications and partners, you will achieve greater control and simplify IT management, so your IT teams can focus on innovation. Managed services can be a great way to take advantage of the latest and greatest security technologies while relieving internal teams' workloads, but it's important to carefully select and rationalize vendors when possible. Be sure to choose a trusted partner who not only understands your unique challenges but can amplify the capabilities of your IT teams with cybersecurity services, so you can maintain efficiency as you evolve.

When setting out to streamline your operations without downgrading your defenses, consider these questions:

- Has your organization ensured the appropriate level of redundancy in its security capability?
- Does your organization use AI tools to help with detection, response and recovery?
- Does your organization routinely scrutinize its internal and third-party security providers to ensure their effectiveness and value?

A do-from-anywhere world requires smarter security

Distributed data, do-from-anywhere work models, multi-cloud environments, and as-a-service sourcing present significant uncertainty in the modern cybersecurity landscape. Human error can compound that uncertainty. As a CIO, it's up to you to make sure your cybersecurity accounts for each of these uncertainties.

A modern approach to cybersecurity is vital. Your cybersecurity apparatus needs to be prepared to protect your data and systems, reduce the impact of cyberattacks and scale cybersecurity measures effectively while minimizing added complexity.

Dell Technologies is committed to helping you plan, protect, detect, respond to and recover from cyberattacks so you can fully dedicate your teams and resources to what matters: driving your business forward.

Learn more at dell.com/cio

Learn more about the Breakthrough study at dell.com/breakthrough

Learn more about our security solutions at: dell.com/en-us/dt/solutions/security/index.htm

Source: Based on Dell Technologies "The Breakthrough Study" April 2022. Fieldwork conducted August-October 2021. Research and Analysis conducted by Vanson Bourne on behalf of Dell Technologies.