TANIUM

How to Avoid Disruption by Bridging the Resilience Gap

Table of Contents

Executive Summary

Modern IT teams must maintain compliance with an evolving set of regulatory standards, track and secure sensitive data across endpoints, and manage a dynamic inventory of physical and cloud-based assets, all while fulfilling an increasingly common executive mandate to make technology an enabler for business growth. But balancing these priorities often cause significant challenges and trade-offs for many business and IT leaders.

According to our latest study:

- Over 94% of CIOs and CISOs said they have to make compromises in how well they are able to protect their organizations from disruptions to technology, including cyber threats and outages.
- A lack of visibility across endpoints – laptops, servers, virtual machines, containers, or cloud infrastructure – is preventing organizations from making confident decisions, operating efficiently, and remaining resilient against disruptions.
- Almost a third (32%) of respondents said that departments and business leaders work in silos, leaving them with a lack of visibility and control over IT operations.
- This lack of visibility has directly affected the business, with the majority (80%) of CIOs and CISOs having found out that a critical update or patch they thought had been deployed had not actually updated all devices, leaving the business exposed as a result.

To understand exactly how organizations are addressing technology-based disruption, Tanium commissioned a study in two phases. The first surveyed over 4,000 business decision-makers working in the United States, United Kingdom, Germany, France and Japan, to understand the barriers to achieving resilience against disruption. The second explored the IT security and operational trade-offs that more than 500 CIOs and CISOs face when it comes to protecting their business from a growing number of cyber threats and other disruptions.

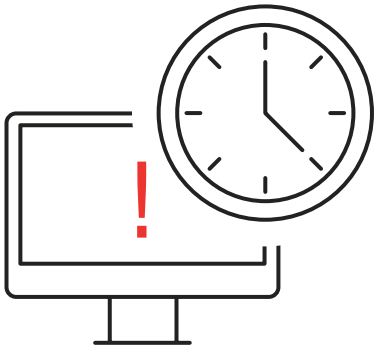
Both phases of our study clearly show that a new approach is needed to achieve visibility and control of distributed, dynamic IT environments. In this report, we look at the ways IT teams could adapt their technical and cultural practices to stay resilient.

Why is resilience important?

The global volume of cyber-attacks rose 63% last year according to some estimates. It's easier than ever for adversaries to access and build tools that attack the weak points in enterprise infrastructure and harder for businesses to have oversight over them all. But cyber-attacks are only one form of disruption for modern IT teams. Outages, for example, are another form of disruption that stems from complex legacy infrastructure, poor patching hygiene and other factors.

Keeping up with these myriad challenges can feel like a game of Whac-a-Mole, with organizations investing in multiple tools that don't integrate effectively and require multiple management consoles just to be effective. Many organizations rely on more than 20 different point products just to manage their IT infrastructure and attempt to plug security holes against disruption.

Our Resilience Gap study found that business decision-makers believe that making technology resilient to disruption should be core to their firm's wider business strategy. However, only around half (54%) say that it definitely is.



$700 billion

is lost every year as a result of **IT downtime** in North American businesses

Digital-oriented businesses must be prepared to safeguard assets, protect customers, maintain brand reputation, optimize workflows and mitigate the likelihood of data being compromised. Regardless of the cause, a business grinding to a halt, even for a matter of minutes, can affect customer confidence, brand equity and ultimately revenue -- not to mention productivity. North American businesses alone are losing $700 billion every year to IT downtime.

Let's look at what seems to be holding businesses back from achieving a more resilient posture.

Barriers to resilience against disruption

The most common challenges referenced by business decision-makers in our study include the following:

34%

cite their organization's growing complexity

33%

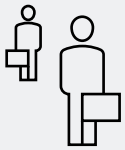
say the issue lies with the hackers being more sophisticated than IT teams

24%

cite poor visibility of attacker entry points

21%

said they don't have the skills needed within the company to accurately detect cyber breaches in real-time



20%

cite siloed business units

Beyond the more technical challenges noted above, their CIO and CISO counterparts highlight broader pressures that cause them to make compromises. Respondents stated that pressure to "keep the lights on" was the biggest barrier (33%), followed by a focus on implementing new systems (31%), restrictions imposed by legacy IT systems (26%), and internal politics (23%).

A lack of understanding of the need for resilience among other leaders across an organization was also identified as a key factor causing CIOs and CISOs to make compromises in their efforts to avoid disruption. Almost half (47%) of the CIOs and CISOs surveyed said that they face challenges due to the fact that other business units do not grasp how important technology resilience is to the company. About 40% said issues arise as other business units prioritize their customer work over security protocols.

IT security and operational trade-offs

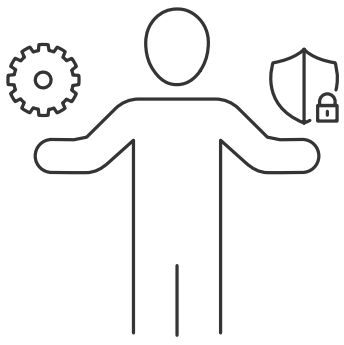
Without visibility of endpoint and infrastructure data in real-time, IT and security leaders will struggle to both keep complex systems running smoothly and defend them against the range of threats plaguing modern businesses. Security personnel, IT operations teams and other business unit leaders must be fully aligned and working from a common set of actionable data.

Our study showed that 9 out of 10 CIOs and CISOs (94%) have made trade-offs among core elements of security hygiene and IT operations effectiveness, including when it comes to critical application updates and patches. For example, 81% of CIOs and CISOs said they have refrained from making an important security update or patch, due to concerns about the impact it might have on business operations, while over half (52%) have done this on more than one occasion. With a large percentage of breaches tied in some way to patching problems, organizations can't afford to hold back critical patches.

But patching is just one example of how a lack of visibility across endpoints – laptops, servers, virtual machines, containers, or cloud infrastructure – is preventing organizations from making confident decisions, operating efficiently, and remaining resilient against disruptions. Almost a third (32%) of respondents in the study claim that departments and business leaders work in silos. And a majority (80%) of CIOs and CISOs have found out that a critical update or patch they thought had been deployed had not actually updated all devices, leaving the business exposed as a result.

9 in 10

CIOs and CISOs (94%) said that they make trade-offs among core elements of security hygiene and IT operations effectiveness, including when it comes to critical application updates and patches.



The impact of a lack of resilience and visibility

If technology stops running due to disruption, the business will, too — with potentially disastrous consequences for sales, customer confidence, brand equity, and business productivity.

Many CIOs and CISOs worry about the impact of not being resilient against disruptions and cyber threats. Over a third of respondents (35%) are concerned about the potential loss of customer data due to the need to make security compromises, while a third (33%) worry about a loss of customer trust. A quarter (25%) of respondents said that the company being unable to comply with current regulations was also a concern.

Many business decision makers also struggle with identifying the financial risk of disruption. A third (33%) of business decision-makers surveyed said they could not or did not know if they could calculate the impact of a cyber breach on indirect cost from lost revenue and productivity. Over a quarter (28%) said the same for working out the financial costs incurred by response efforts.

35%

are concerned about the potential loss of customer data

33%

worry about a loss of customer trust

25%

said that the company being unable to comply with current regulations was also a concern

What does a resilient organization look like?

As organizations look to build a strong security and compliance culture, it is essential that IT operations and security teams unite around a common set of actionable data for true visibility and control over all of their computing devices. This will enable them to prevent, adapt and rapidly respond in real-time to any technical disruption or cyber threat.

A resilient organization successfully exhibits the following:

1. **Unified response:** Resilient organizations have their IT security, operations and risk teams working together to simplify and secure their IT environment, source reliable data to make confident decisions, and be agile and effective in the face of constant growth and change.

2. **Full grasp of the IT environment:** The CIO or CISO of a resilient organization maintains accurate real-time endpoint visibility. They can answer accurately how many unpatched devices are on a network and empower employees with real-time data, to act quickly and counteract the growing volume of sophisticated security threats.

3. **Decluttered infrastructure:** One of the most cited issues throughout the WannaCry incident was the challenge of updating operating systems in an environment laden with legacy apps. A resilient organization is one that isn't hampered by multiple legacy and disparate tools to operate.

4. **Eliminated Fragmentation:** The scale of today's networks and the proliferation of endpoint devices - be they laptops, servers, virtual machines, containers, or cloud infrastructure - introduces complexity and risk for every organization. The fragmented array of legacy or alleged endpoint platforms and narrow point solutions also leaves organizations blind and unable to effectively operate and secure their business. In resilient firms, IT security and operations teams are united around a common set of actionable data for true visibility and control over all computing devices, enabling them to prevent, adapt and rapidly respond to any technical disruption.

5. **Educated employees:** By various estimates, up to 83% of ransomware attacks originate when an employee clicks on a malicious link, opens an infected attachment, or visits a compromised website. Those firms which invest in ongoing training for employees to protect against phishing and other forms of cyberattacks are the most resilient.

Research Methodology

Tanium commissioned independent market research specialist Censuswide to undertake the research. A total of 4,022 business decision-makers and 504 frontline CIOs and CISOs were interviewed from July to October 2018, in the United States, United Kingdom, Germany, France, and Japan. The respondents were from organizations with at least 1000 employees and could be from any sector.

Tanium offers a proven platform for endpoint visibility and control that transforms how organizations manage and secure their computing devices with unparalleled speed and agility. Many of the world's largest and most sophisticated organizations, including half of the Fortune 100, top retailers and financial institutions, and four branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruptions. Tanium recently ranked 4th on the Forbes list of "Top 100 Private Companies In Cloud Computing For 2018" and 55th on FORTUNE's list of the "100 Best Medium Workplaces". Visit us at www.tanium.com or follow us on Twitter at @Tanium.

tanium.com

@Tanium

info@tanium.com