TANIUM

Whitepaper

How IT Resilience Gaps Impact Your Business

Executive Summary

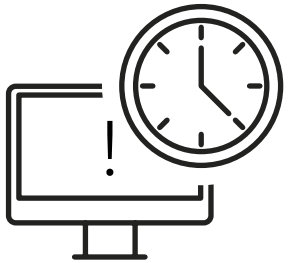
Modern IT teams feel pressure from all directions. They must maintain compliance with an evolving set of regulatory standards, track and secure sensitive data across endpoints, and manage a dynamic inventory of physical and cloud-based assets, all while fulfilling an executive mandate to make technology enable business growth. Balancing these priorities often causes significant challenges for many business and IT leaders, leading to gaps in overall resilience.

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

According to our Resilience Gap Study:

- **IT leaders are making trade-offs:** More than 94 percent of CIOs and CISOs said they must make compromises in how well they are able to protect their organizations from disruptions to technology, including cyber threats and outages.
- **Teams are working in silos:** Almost a third (32 percent) of respondents said that departments and business leaders work in silos, creating a lack of visibility into and control over IT operations.
- **Visibility gaps are driving serious challenges:** 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.
- **Poor visibility leaves businesses exposed:** This lack of visibility directly affects the business, with the majority (80 percent) of CIOs and CISOs realizing that a critical update or patch they believed deployed had not actually updated on all devices, leaving the business exposed.

Both phases of our study clearly show that a new approach is needed to achieve visibility and control of distributed, dynamic IT environments and close gaps in resilience. What follows is a look at the ways IT teams can adapt their technical and cultural practices to stay resilient.



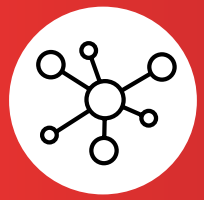
$700bn

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

Here is what is holding businesses back.

Barriers to resilience against disruption

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



34%

cite their organization's growing complexity

33%

say hackers are more sophisticated than IT teams

24%

cite poor visibility of attacker entry points

21%

say the company lacks the necessary skills to accurately detect cyber breaches in real-time

20%

cite siloed business units

Further, CIOs and CISOs highlight broader pressures that cause them to make compromises. Respondents stated that pressure to "keep the lights on" was the biggest barrier (33 percent), followed by a focus on implementing new systems (31 percent), restrictions imposed by legacy IT systems (26 percent), and internal politics (23 percent).

IT security and operational trade-offs

Without visibility into 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 that plague 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 if they are to succeed.

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

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.

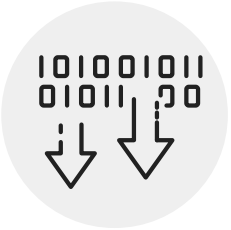
But patching is just one example of how a lack of visibility across endpoints—laptops, servers, virtual machines, containers, or cloud infrastructure—is preventing organizations from making confident decisions, operating efficiently, and remaining resilient against disruptions. Almost one third (32 percent) of respondents in the study claim that departments and business leaders work in silos. And a majority (80 percent) 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.

A lack of understanding of the need for resilience among other leaders across the organization was also identified as causing CIOs and CISOs to make compromises in their efforts to avoid disruption. Almost half (47 percent) of the CIOs and CISOs surveyed said that they face challenges brought on by other business units not grasping how important overall resilience is to the company. About 40 percent said issues arise when other business units prioritize their customer work over security protocols.

The impact of a resilience gap

If disruption causes technology to stop running, the business will stop, too. That's why so many CIOs and CISOs worry about the impact of not being resilient. Thirty-five percent of respondents are concerned about the potential loss of customer data that results from the need to make security compromises, and one third (33 percent) worry about a loss of customer trust. A quarter (25 percent) of respondents said a further concern is the company not being able to comply with current regulations.

Many business leaders also struggle with identifying the financial risk of disruption. A third (33 percent) 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. More than a quarter (28 percent) said the same for working out the financial costs incurred by response efforts.



35%

of IT leaders 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 their computing devices. This will enable them to prevent, adapt, and rapidly respond in real-time to any technical disruption or cyber threat.

Here are five signs that your business is on the path to becoming truly resilient:

1. **Your business has adopted a unified approach to endpoint management and security:** Resilient organizations have their IT security, operations, and risk teams working together to simplify and secure the IT environment, source reliable data to make confident decisions, and be agile and effective in the face of constant growth and change.

2. **Your business has a 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 to counteract the growing volume of sophisticated security threats.

3. **Your business has prioritized decluttering your infrastructure:** A resilient organization is one that isn't hampered by multiple and disparate legacy tools. Updates to operating systems in an environment laden with legacy apps are a tremendous challenge, as WannaCry and other major security incidents from recent years revealed.

4. **Your business has eliminated fragmentation:** The scale of today's networks and the proliferation of endpoint devices introduces complexity and risk across the board. The fragmented array of legacy endpoint platforms and narrow point solutions also leaves organizations blind and unable to effectively operate and secure the 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. **Your business has invested in employee education for IT security best practice:** By various estimates, up to 83 percent of ransomware attacks originate when an employee clicks on a malicious link, opens an infected attachment, or visits a compromised website. Those firms that 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 used in this report. 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 industry sector.

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With the unprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

tanium.com

@Tanium

info@tanium.com