

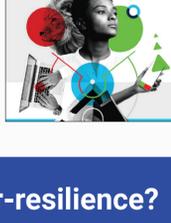
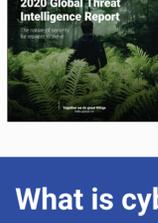
Are you ready for anything?

Events of 2020 have highlighted that cyber-resilience is more important than ever.

Security insights from NTT and Cisco.

Data-driven insights

Security insights from NTT and Cisco's annual security thought leadership reports



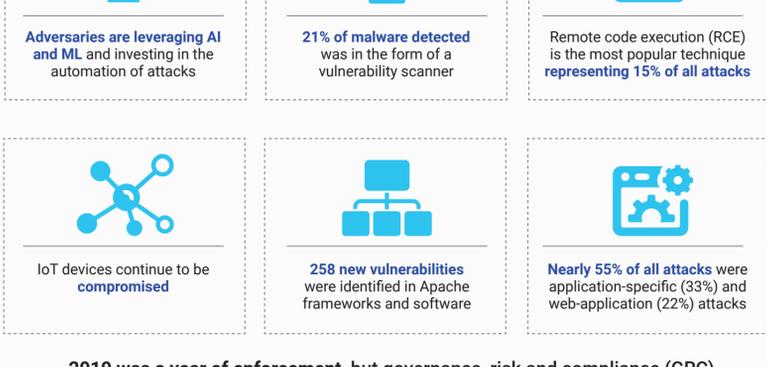
What is cyber-resilience?

Cyber resilience is the ability to continuously maintain business as usual through successful defense against persistent threats and ever-evolving sophisticated attacks. This includes a fluid, flexible approach to preventing attacks, detecting and correcting breaches faster, and minimizing the impact of a breach.

Attack volumes increased between 2018 and 2019 due to overwhelming success of tools such as web shells, exploit kits and targeted ransomware, plus the addition of AI, ML and automation to ramp effort.

Changing threat landscape

Attacks are evolving, making them harder to combat, and businesses struggle with poor practices and overall security hygiene. Our recent analysis shows:



2019 was a year of enforcement, but governance, risk and compliance (GRC) is becoming more complex and challenging to navigate.

Source: NTT Ltd. Global Threat Intelligence Report 2020

Old vulnerabilities still a target

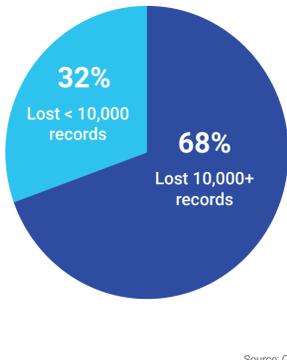
We continue to see attackers focus on older vulnerabilities despite patch availability, because organizations aren't following best practices.¹

46% of organizations in 2019

had an incident caused by an unpatched vulnerability. (up from 30% the year before²)

Those with a major breach due to an unpatched vulnerability experienced higher levels of data loss.

Unpatched vulnerability



Other reasons



Source: Cisco 2020 CISO Benchmark Survey

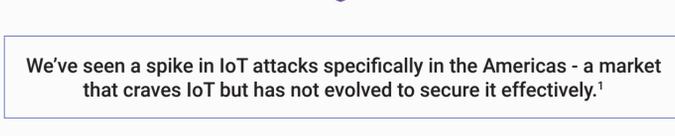
Growing security challenges are made worse by massive change, distributed environments and workloads, and remote and mobile trends.

More IoT devices connect everyday
By 2025, there will be **41.6B CONNECTED IOT DEVICES**³

Workloads and apps are shifting to the cloud
80% OF ENTERPRISE workloads will move to cloud by 2025⁴

Users work anywhere across many devices
By 2025, nearly **80% of ALL IP TRAFFIC** will come from wireless and mobile devices⁵

Direct internet access at distributed branches
By 2023, the SD-WAN market is expected to **GROW 74% CAGR** from 2018 for explosive branch DIA⁶



We've seen a spike in IoT attacks specifically in the Americas - a market that craves IoT but has not evolved to secure it effectively.¹

Complexity leads to burnout and weaker defenses

The growing complexity of IT and the threat landscape has driven organizations to turn to a variety of vendors to bolster security. This has led to greater complexity for security teams and an overabundance of alerts and signals to sort through.

42%

of businesses suffer from cybersecurity fatigue and have given up on proactive defense

96%

of fatigue sufferers say managing a multi-vendor environment is challenging

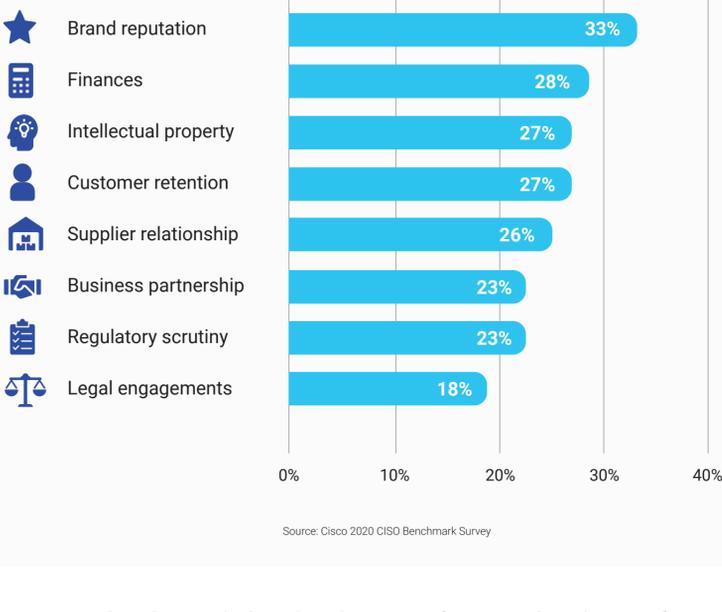
93%

of fatigue sufferers receive more than 5,000 alerts every day

Source: Cisco 2020 CISO Benchmark Survey

Where we feel the pain from a security breach

Impact to finance: the average total COST of a DATA BREACH is \$3.92M USD⁷

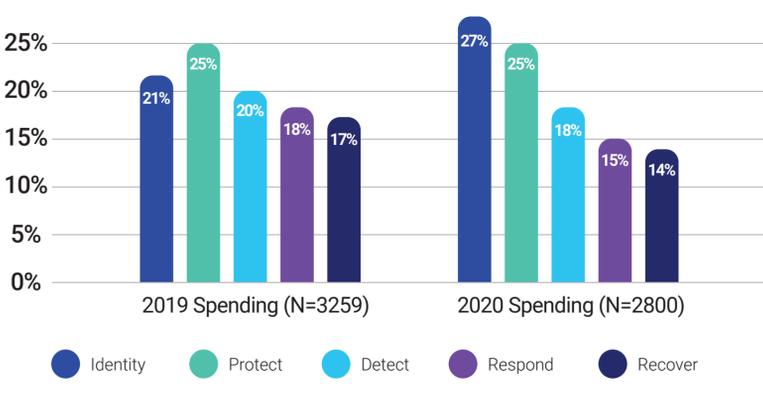


Source: Cisco 2020 CISO Benchmark Survey

Damage to brand rises. The hit to brand reputation from major breaches rose from 26% to 33% in the last three years. It's crucial to include crisis communications planning in your incidence response plan. **61% of organizations have seen their credibility rise** when they voluntarily disclose a major breach.²

Become proactive and predictive

A recent shift in spend shows a desire to become more proactive and predictive, with a rise in expenditures to better identify threats. The overall trend shows **organizations are spending more on prevention versus being reactive.**



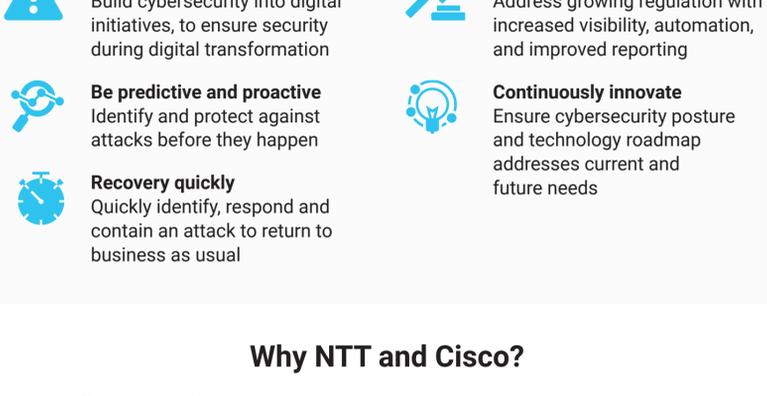
Source: Cisco 2020 CISO Benchmark Survey

Identify, mitigate and respond with NTT and Cisco

Complexity and cybersecurity fatigue are straining resources. Turning to a trusted partner can help. **34% of businesses are outsourcing incident response services and 36% are using third-party services to analyze compromised systems.²**

NTT and Cisco deliver best of breed technology and services to improve an organization's security posture, mitigate risks, and respond to incidents.

Together we help clients:

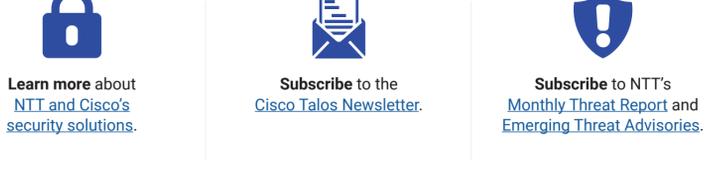


Why NTT and Cisco?

For more than 28 years, we've worked together to help organizations around the world harness the power of technology to innovate.



How can we help you go further?



Sources:
 1. NTT Ltd. Global Threat Intelligence Report 2020
 2. Cisco 2020 CISO Benchmark Survey
 3. IDC Forecast: "The Growth in Connected IoT Devices", June 2019
 4. Oracle's Top 10 Cloud Predictions 2019
 5. https://cybersecurityventures.com/mobile-security-report-2017/
 6. Apps Run The World: Top 10 SD-WAN Software Vendors, Market Size and Market Forecast 2018-2020*, Dec 2019
 7. Ponemon, Cost of a Data Breach Study, 2019