SPOTLIGHT

Sponsored by: Tata Communications

Cyber-risks have graduated to the highest levels of significance and changed the buyer persona for cybersecurity. No longer confined to IT, cybersecurity has become a boardroom concern, evolving to prioritize cyber-resilience. This Spotlight looks at how organizations can manage this strategic business imperative.

Building Blocks of Cyber-Resilience

April 2024

Written by: Cathy Huang, Research Director, and Craig Robinson, Research Vice President, Security Services, IDC

Introduction

Greater attention from the C-suite to cybersecurity reflects the gravity of the situation. Cyberthreats and increased regulatory compliance continue to rank high on the list of top business risks, reclaiming the number 1 spot in 2024 (see Figure 1).

FIGURE 1: ***Top 3 Risks Impacting Business***

Source: IDC Worldwide CEO Sentiment Survey, 2022 & 2023

For the chief information security officer (CISO), whose role was nonexistent two decades ago, every high-profile security breach reported is a reminder of the havoc that can be wreaked by the failure to implement security best practices. In most cases, organizations have inadequate backup procedures in place, exacerbating financial losses and prolonging recovery efforts.

Incidents like the devastating NotPetya attacks on Maersk in 2017 and the brute-force techniques used to gain access to the networks of Atlanta's City Hall in 2018 are a call not only to address vulnerabilities in digital systems, but also proactive security measures and leadership.

AT A GLANCE

KEY STATS

- Most organizations (87%) have experienced disruptions lasting from a few days to as long as a few weeks.
- Close to 40% of organizations across the globe are just starting to execute on their plans or figuring out their cyber-resilience strategy.
- Only 13% of organizations have experienced business disruptions of less than one day because of cybersecurity incidents.

WHAT'S IMPORTANT

- Cyberthreats and regulatory non-compliance have been a top business risk between 2022 and 2024.
- The very existence of digitally transformed organizations may depend on their capabilities to withstand a cyberattack and quickly restore to a viable operating status.

Source: IDC's Worldwide Security Services Primary Research

Organizations that prioritize cyber-resilience can ensure that all critical systems and services remain accessible, even in the face of major disruptions brought on by ransomware, volumetric distributed denial-of-service (DDoS) attacks, insider threats, business email compromise (BEC) attacks, supply chain attacks, and others.

Cyber-Resilience: Business Enabler and Strategic Differentiator

Companies that have successfully achieved digital transformation realize that their very existence may depend on their capability to withstand a cyberattack and bring about a quick restoration of a viable operating status. Taking a proactive approach to cybersecurity is an effective enabler and strategic differentiator for businesses. Cyber-resilience goes hand in hand with other dimensions of organizational resilience, such as financial resilience and operational resilience (see Figure 2). It is an integral part of the overall resilience to withstand and thrive in an increasingly interconnected digital world.

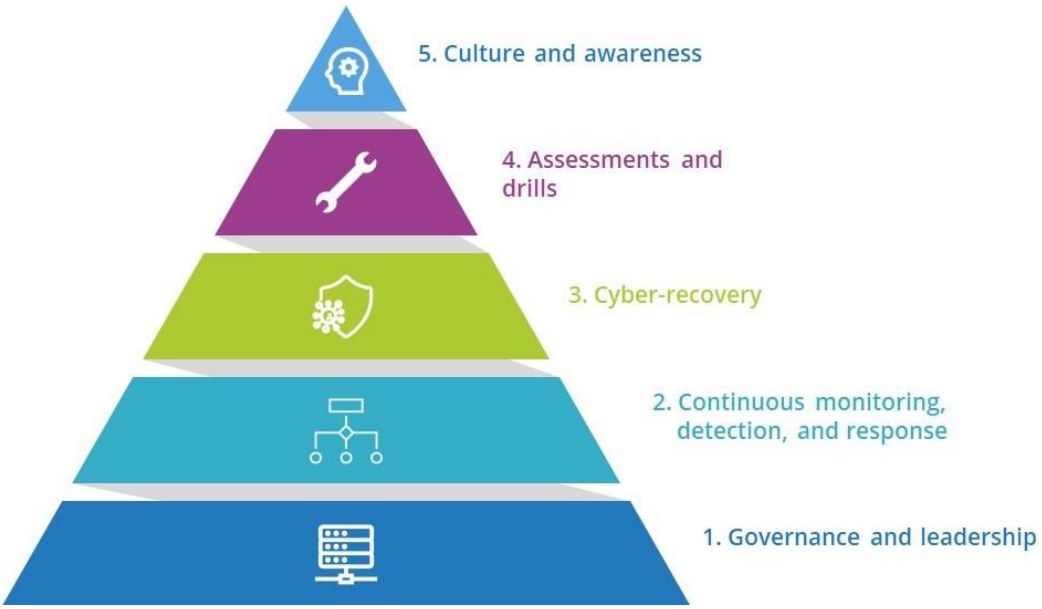
FIGURE 2: ***Cyber-Resilience: One of the Top 3 Risk Areas to Plan For***

Source: IDC, 2024

Operationalizing Cyber-Resilience

IDC defines a cyber-resilient organization as one that has the capability to minimize damage during a cyberattack and quickly return to performing minimal essential functions needed to stay operational. A cyber-resilience strategy should be comprehensive, helping organizations to effectively manage the risk of cyberthreats, including the processes and technologies to prevent, detect, respond to, and recover from cyber incidents (see Figure 3).

FIGURE 3: ***Five Building Blocks for Operationalizing Cyber-Resilience***



Source: IDC, 2024

Foundations — Governance and Leadership

This dimension serves as the capstone for all other dimensions, with lines of business (LoBs), CISO, chief information officer (CIO), and the broader C-suite identifying primary objectives, budget, and alignment between the cyber-resilience strategy and the overall business objectives for future success.

It is critical to set the vision and strategy, fostering a culture of overall organizational resilience, managing risks, building an effective decision-making approach to achieve multidimensional resilience enabling the organization to embrace and respond to challenges. Implementing a governance framework involves aligning organization policies, procedures with strategic objectives, establishing clear accountability and responsibilities. Common ones include the NIST cybersecurity framework, COBIT or ISO/IEC 27001.

The zero trust model is becoming increasingly important to an organization's overall security posture and resilience. In addition to limiting the 'blast surface' of an attack, its proactive attributes improve the resilience of an organization by providing granular control over access to critical systems and data. That is why a growing number of regulations (e.g., NIST SP800-207 or the U.S. Executive Order) have explicit recommendations to implement a zero trust strategy or principles.

Continuous Monitoring, Detection, and Response

This dimension is a core pillar to support an organization’s security posture and effectively achieve cyber-resilience level. Often, organizations follow a framework and set policies, standards, and procedures defining cybersecurity roles and

responsibilities. They then implement and manage in-house cybersecurity monitoring mechanisms and other necessary controls like firewalls (FWs), intrusion detection systems (IDS), web application firewalls (WAF), identity access management (IAM), endpoint detection and response (EDR), and security information and event management (SIEM). Alternatively, they engage a trusted managed security services/managed detection and response provider to perform 24x7 monitoring, managed detection, and response services to protect the enterprise.

Continuous monitoring gives organizations real-time visibility into their operations and external ecosystems, enabling them to expedite problem solving when they need to respond to unexpected disruptions. Moreover, a growing number of regulations across countries require mandatory incident reporting and even encourage organizations to join voluntary information and threat intelligence sharing arrangements.

Essentially, the cyber-resilience cycle of identify, protect, detect, respond, and recover can validate an organization's cybersecurity portfolio of services and products, and related processes, such as:

- Set up cybersecurity monitoring mechanisms for detecting and responding to cyberincidents.
- Consider collecting telemetry from a broad range of security controls, such as network, endpoint, identity, SIEM, mobile, cloud, operational technology (OT), and Internet of Things (IoT).
- Leveraging behavior analytics, machine learning, and artificial intelligence (AI) to identify the indicators of attack (IOAs).

Cyber-Recovery

Every click, swipe, and interaction contributes to an unprecedented surge in data generation, replication, analysis, and storage. The growth of data necessitates a paradigm shift in the approach to backup and recovery. A cyber-recovery plan outlines how an organization will recover from a cyberattack, including steps to identify and recover the systems and data that are essential for a business to operate.

The cyber-recovery plan often goes hand in hand with a cyber incident response plan. The incident response plan states the step-by-step procedures to be followed in the event of a cyber incident, including roles and responsibilities, incident detection, containment, and mitigation processes, reporting, communication, root cause analysis, and recovery steps.

Key technologies/tenets of cyber-recovery solutions look to implement the 3-2-1-1 best practice rule:

- Three copies of your data — one primary and two backups
- Two copies stored locally on two formats
- One copy stored offsite in the cloud or secure storage
- One copy live in immutable storage

Security Assessment and Drills

When the European Union introduced its Digital Operational Resilience Act (DORA) for its financial entities and their ICT partners, it gave organizations the opportunity to review the status of their systems and turn compliance into an effective

strategy for cyber-resilience. The adherence to operational resilience, cybersecurity, and data protection requirements plays a vital role in safeguarding brand reputation, fostering a trusted customer and partner ecosystem.

In a study that IDC published in May 2023 on cyber-resilience, only 20% of surveyed organizations said that they constantly test and optimize their cyber-resilience plan. The majority of organizations have a plan in place but test it infrequently, or never test it.

Therefore, it is important to perform regular information security risk assessments and cybersecurity drills, analyzing and evaluating the status and identifying potential gaps. A common list of activities worth testing on a regular basis:

- Disaster recovery drills for failover and failback
- Cybersecurity maturity assessment
- Compliance readiness services, e.g., General Data Protection Regulation (GDPR), Personal Data Protection Act (PDPA), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST)
- Verify software, firmware, and information integrity through software/app testing
- Vulnerability assessment and penetration testing
- Red teaming services

Culture and Awareness Training

Cyber-resilience is not only about investing in IT security. It is a moving target — what is considered resilient today, might become obsolete in the future with the adoption of new technologies. It is critical to cultivate a cyber-aware and resilient culture within the organization, which will help it to respond to future challenges.

IDC research shows that the top 2 sources of the initial compromise in ransomware incidents are directly related to **users' internet behaviors** (see Figure 4). In a drive-by compromise, adversaries gain access to their target's systems by taking advantage of users' normal course of web browsing. Employees can be an easy target due to a lack of awareness and the use of social engineering by cybercriminals to deceive them into clicking on malicious links and attachments in phishing email.

FIGURE 4: ***Top 5 Most Significant Sources of the Initial Compromise From Ransomware***

1.	Drive-by compromise (adversaries gain access over the normal course of web browsing)
2.	Clicked on a malicious URL or opening a malicious attachment in a phishing email
3.	Supply chain attacks (e.g., SolarWinds, PC Cleaner, or Kaseya)
4.	Malicious access which leveraged a compromised credential
5.	Malware stored on peripheral devices or removable media inserted into a

Source: IDC Future Enterprise Resiliency & Spending Survey, Wave 11, December 2023

Security awareness training helps to educate users to understand, identify, and ultimately reduce human error when it comes to cyberthreats. One of the most popular ways to test people's response to cyberthreats is to simulate an attack. Hence, there is a growing demand for simulation-based phishing tests and ransomware attacks — engaging, interactive, and educational.

Business Outcomes of Achieving Cyber-Resilience

A cyber-resilience strategy should be comprehensive, helping organizations to effectively manage the risk of cyberthreats, including the processes and technologies to prevent, detect, respond to, and recover from cyberincidents.

Pairing a cybersecurity program with strong cyber-recovery capabilities enables the organization to have the necessary cyber-resilience during and after a cyberattack. Cybersecurity and recovery investments provide a great strategic advantage to an organization's digital success because it allows the organization to go into new ventures with a high level of confidence.

Key business outcomes include:

- **Reduction in unplanned downtime:** One of the core tenets of cyber-resilience is the ability to restore the minimal viable capabilities needed to function. Effective cyber-resilience programs allow for a timely recovery during or after a cyberattack, thereby reducing the total cost of the attack.
- **Avoid repeated cyberattacks:** Successful cyberattacks can be catastrophic. But what's worse is when an attack gains a second life because of an inadequate incident response or when malware is reintroduced into production systems from a recovered backup.

- **Quick claims processing:** In the event of a cyberincident, organizations with higher levels of cyber-resilience are better positioned to detect, contain, and recover from the incident quickly. This can lead to faster claims processing and reimbursement from insurers. Insurers may offer lower premiums to organizations with high levels of cyber-resilience too.
- **Reduction in business and operational risks:** Identifying the key assets that are necessary for an organization to perform their model-view-controller (MVC) pattern should result in the proper allocation of the cybersecurity budget to protect these assets. Increased visibility and practicing recovery capabilities for these key assets will lower the risk of permanently losing them.
- **Lower risk of incurring fines and non-compliance:** Raising the organizational cybersecurity maturity to the level where cyber-resilience is taken seriously also implies that other governance, risk, and compliance (GRC) activities are actively being pursued. This reduces the risk of additional fines for non-compliance.

Considering Tata Communications' Cybersecurity Offerings

Tata Communications is a global communications, connectivity, and security services provider, with its headquarters in India. It owns one of the largest subsea fiber networks, underpinning the internet backbone and carrying about 30% of the global internet routes. Tata Communications aims to be a premier provider of cybersecurity services and a one-stop partner for managing cyber-risks globally.

Tata Communications approaches cyber-resilience with its Anticipate – Defend – Respond (ADR) methodology, focusing on predictive security and assured recovery. Its cybersecurity portfolio is built on three pillars of Advisory, Transform, and Manage, including capabilities across endpoints to cloud, namely:

1. Advanced network security — including security service edge (SSE), DDoS protection services, perimeter edge security

2. Cloud security — including cloud native security, third-party cloud security controls including data loss prevention (DLP) and IAM, CNAPP

3. Cyberthreat detection and response — including managed and captive security operations center (SOC), managed detection and response (MDR), threat hunting, managed SIEM, EDR, NDR

4. Security assessment and consulting services — including vulnerability assessment, data discovery and classification, cybersecurity maturity assessment, phishing simulation and security awareness services.

Tata Communications has helped its clients achieve the following business benefits:

- Automation of incident response process for unified visibility against an evolving threat landscape
- Analyzing anomalies in user behavior to detect threats
- Detecting threats in real time with IoAs that analyze code execution, command and control (C&C) communications and lateral movement

- High confidence indicators of compromise (IOC) augmented by comprehensive scrutiny of its Netflow data (25 million records/minute), and reducing false positives
- Lower total cost of ownership (TCO) with improved operational effectiveness and efficiency of SOC operations with integrated log monitoring, security analytics and native SOAR
- Reducing detection and response time for critical assets ensuring business continuity
- Improved security posture with comprehensive visibility and greater experience

Opportunities

Stricter security measures mandated by the emerging regulatory frameworks continue to shape the development of the cybersecurity field and push security vendors to address the challenges their clients face. Tata Communications has an opportunity to stand out by aligning its compliance-readiness services to specific cyber-resilience requirements for its clients.

Conclusion

Instead of asking "Are we safe?", the right question IT and cybersecurity leaders should ask themselves is: "Are we cyber-resilient?"

The growing reliance on technology by organizations to improve customer experience, support business operations, and enable supply chain management has accelerated the need for cyber-resilience. Tata Communications' security offerings present a viable option in the market for organizations across all maturity levels to build their cyber-resilience imperative.

About the Analysts

Cathy Huang, *Research Director, Security Services Worldwide*

Cathy Huang is the Research Director for IDC's WW Security Services research practice. In her role, she collaborates with other worldwide and regional analysts to develop a set of thought leadership and actionable research for IT buyers and suppliers. Specifically, she develops core research around managed security services, security consulting, and integration services within the program. Cathy also incorporates IDC's Future of Trust and other FoX agenda to drive new research such as cloud security services and secure edge services for the program. She brings a wealth of security and services expertise and knowledge to the position. She draws on her deep domain expertise across a broad range of ICT segments to support any custom or advisory work with regard to security services.

Craig Robinson, *Research Vice President, Worldwide Security Services*

Craig Robinson is a Research Vice President within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include Managed Detection and Response services, Cyber-Resilience, and Incident Readiness & Response services. Craig delivers unparalleled insight and analysis, leveraging his unique practitioner experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research and guidance to vendors, service providers and clients worldwide.

MESSAGE FROM THE SPONSOR

Holistic cybersecurity solutions mitigate risks

"Today's organizations strive for holistic cybersecurity solutions that enable them to predict, safeguard against, counteract, and rebound from cyberthreats with confidence. Fostering resilience starts by foreseeing potential risks through ongoing monitoring and analysis, and staying ahead of emerging threats. Cutting-edge technologies and top-tier expertise are crucial for ensuring robust defense against modern attacks. In case of a cyberincident, swift automated response helps contain the threat and mitigate operational disruptions. By implementing meticulous recovery plans, such as data backups and system reinstatement, businesses can minimize downtime and maximize resilience. With Tata Communications as your cybersecurity ally, you can navigate the digital terrain with resilience and peace of mind." — Vaibhav Dutta , AVP MSS Products & Engineering, Tata Communications

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com