CyberTalk.org

A CISO's Guide to Resilience

As Enabled through Cybersecurity

TABLE OF CONTENTS

INTRODUCTION

Imagine this: In the tech-savvy town of Techville, a company called SecureSystems was well-known for its software products and digital services. The company displaced competitors with top-tier offerings, impeccable customer service, and outstanding quarterly results.

The company was so profitable and had such vast access to large customers that a group of hackers believed that they would profit from extracting company data and intellectual property. What initially appeared as a few minor and isolated cyber incidents began to turn into a full-scale cyber breach.

Adversaries seemed to have uncanny insider knowledge of SecureSystems' vulnerabilities. The firm's cybersecurity team sprung into action, but they had a daunting challenge ahead of them. Hackers exploited a number of vulnerabilities. They also installed multiple backdoors and compromised both phones and email systems. The length of time required to resolve the issues wasn't readily apparent.

As the days turned into weeks, the financial losses began to stack up. SecureSystem's clients, concerned about the security of their data, started to back out of multi-year contracts. SecureSystems' stock price plunged and layoffs became inevitable. The media covered the company's downfall and created a grim narrative.

As SecureSystem's freefall continued, leaders and teams both realized that they hadn't sufficiently prepared for a situation of this magnitude. The company had invested in extensive cyber security (after all, it was a tech firm).
But that wasn't enough. That's where resilience enters the picture.

Failure to pursue cybersecurity and business resilience leaves enterprises vulnerable.

DEFINITION

The National Institute of Standards and Technology (NIST) defines cyber resilience as the ability to **anticipate**, **withstand**, **recover** from and **adapt** to adverse conditions, stresses, attacks or compromises on systems that are used or enabled by cyber security resources.

The goal of cyber resilience is to allow an organization to thrive amidst adverse conditions. Adversity may pertain to cyber security, as in the Techville narrative on the previous page, but it could also pertain to an environmental disaster, a pandemic, or financial volatility, among other things.

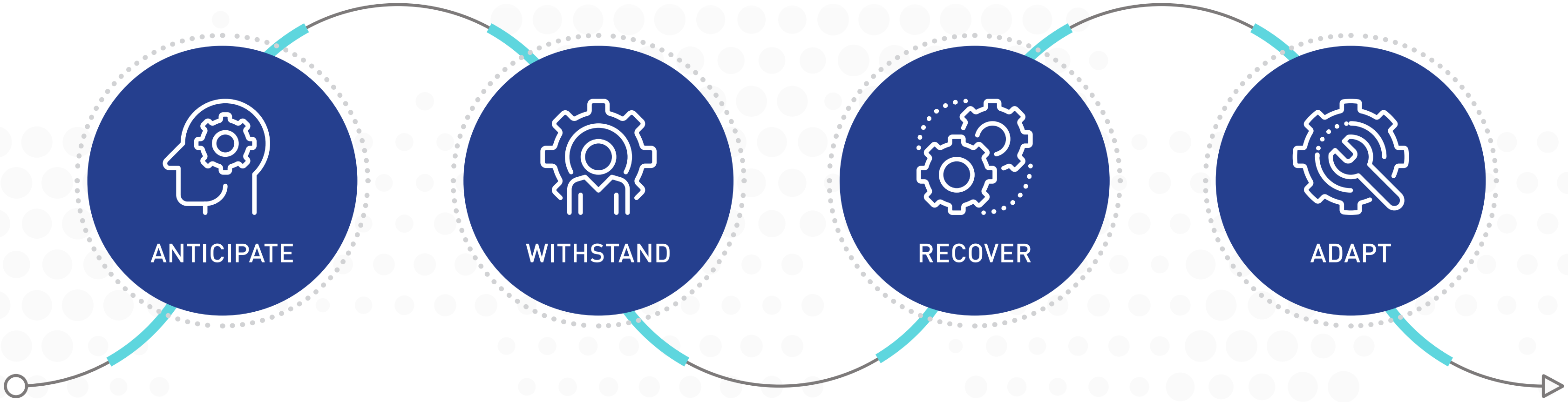
In this eBook, discover how to build greater resilience into your businesses through cybersecurity and cyber resources. Find out about how to execute against a resilience framework and get cutting-edge real-world insights that can prepare you for whatever comes next.

Enhance your risk management model. Get back to business-as-usual after an unanticipated incident—not in days or weeks, but in minutes.

RESILIENCE PILLARS

In striving for greater business resilience as enabled through cybersecurity and cybersecurity resources, NIST's "pillars" can serve as a guideposts.

According to NIST, resilience refers to the abilities to:


ANTICIPATE

WITHSTAND

RECOVER

ADAPT

This eBook offers insights into all four pillars. However, before we dive in, we will briefly cover the importance of **digital transformations** in relation to resilience—an overarching strategy that applies across each of the four pillars.

A core component of building resilience involves developing "shock absorbers" that help sustain enterprise operations, customer outreach and business operations—throughout a crisis.

Digital transformations have a lot to offer from the perspective of resilience. With advanced tools, organizations inherently become more resilient. They also become more agile, increase transparency and obtain stronger data and analytics platforms. In turn, organizations can gain deep insights into data and can make more accurate and effective decisions in difficult situations.

Further, digital transformations can lead to automated processes, streamlined communications and enhanced efficiency—all of which are extremely useful amidst a crisis.

For organizations that aim to increase their business and cyber resilience, pursuing digital transformations is strategic on multiple levels, as they not only offer new capabilities and day-to-day benefits, they can also reinforce resilience efforts.

ANTICIPATE

Move away from a reaction-based crisis response and towards an outlook that anticipates adversity. Here's how:

1 INCIDENT RESPONSE PLANNING AND SCENARIO-BASED PLANNING

Leaders need to create and test versatile and through incident response plans that pertain to a wide spectrum of adversities, risks and high impact events, including those in the cyber domain.

These plans must present clear guidance, outlining every necessary action; from initial containment, communications, and mandated compliance efforts, to full recovery.

As a mandatory supplement to these plans, tabletop exercises and drills can prove invaluable in honing organizational preparedness. Tabletop exercises and drills offer critical insight into overall incident response effectiveness—and they pinpoint areas for improvement. After each exercise, use the "lessons learned" to ensure that you are continuously improving your plan.

Moreover, fostering comprehensive awareness and involvement of all roles and responsibilities from the top down and throughout the organization ensures a seamlessly coordinated and efficient response to adverse events, enhancing overall resilience.

> "Throw a monkey wrench into your IR exercise to simulate unexpected issues that will occur during a real event. For example, render VOIP phones and corporate email unavailable."
>
> – Check Point CISO, Pete Nicoletti

2 Threat Intelligence and Monitoring

Within the cybersecurity space, CISOs must establish robust threat intelligence programs. Corresponding threat intelligence tools should possess the abilities to efficiently gather and analyze vast volumes of data and millions of indicators of compromise (IoCs) on a daily basis. This threat information must automatically be leveraged to prevent issues and protect the business.

In addition to this, cybersecurity professionals can bolster defenses by deploying advanced threat detection systems and adopting security information and event management (SIEM) solutions. Assessing threat intelligence and acting upon related insights rapidly can keep organizations ahead of cyber adversaries.

3 Vulnerability Assessments and Penetration Tests

To stay ahead of cyber threats, cybersecurity leaders should also lead efforts to identify weaknesses in the given organization's security posture. Upon reviewing findings, teams should prioritize remediation efforts based on potential impact, risk probability, and scale of disruption.

Proactive vulnerability management—including patch management, system hardening, cloud and configuration audits—can reduce the cyber attack surface and measurably limit threats.

> "Make sure you are doing "credentialed" vulnerability scans to get the entire picture of your host's issues."
>
> – Check Point CISO, Pete Nicoletti

WITHSTAND

Minimize business disruptions during adverse events. Here's how:

1 Redundancies

For critical systems, implement technological redundancies and segmentation This helps to ensure that failure in one area doesn't lead to widespread business disruptions across a variety of areas.

Redundancies might include backup power sources, data centers, communications channels, and data backups. In the wake of both physical and cyber disasters, these can help ensure data accessibility. Segmentation ensures that there is appropriate, limited and secured connections between systems.

Within your Zero Trust program, segmentation should be second to authentication program maturity efforts.

> In 2022, 62%[1] of companies stated that cyber security incidents had previously affected business operations, sometimes resulting in severe repercussions.

[1] Dark Reading, Cybersecurity Resilience Emerges as Top Priority..., Dec 7th 2022
https://www.darkreading.com/vulnerabilities-threats/cybersecurity-resilience-emerges-as-top-priority-as-62-of-companies-say-security-incidents-impacted-business-operations

2 Supply chain management

Keep lines of communication with suppliers open and establish clear communication channels through which to address supply chain issues—including software supply chain security. Supply chain partners must also be assessed for risks that may be introduced with connections and data sharing agreements. All API's to partners must be secured.

3 Employee preparedness

Across your business, and especially within the cybersecurity team, foster a resilient workforce. One way to do this includes promoting a culture of well-being and mental health support, helping employees contend with the stress stemming from adverse events. This culture needs to be fostered from the top of the organization and on down.

> "In the current high-risk environment of business partner sprawl, with new OS and application zero day vulnerabilities announced every day, cloud deployments popping up weekly, employees working from everywhere, budget challenges and a security workforce shortage, you must assume and plan for a security incident. With the average recovery time near 30 days, a mature, constantly tested resilience plan can reduce this risk area considerably."
>
> – Check Point CISO, Pete Nicoletti

RECOVER

Recovery planning can limit the effects of a cyber security event on a business, its customers and on the market.

Prevention of issues is always preferable, then efficient detection and expedient root cause determination is key in determining the most suitable of recovery strategies.

However, well-designed systems may be able to apply "strategies independently of detection in order to change the attack surface," according to NIST. Essentially, a well-constructed system can potentially automate and offload recovery procedures.

In the event of a cyber breach and in order to recover, a system may revert to an earlier state, revive itself by duplicating critical functions, or may require repurposing existing system elements to support compromised areas.

Implementing an incident response management plan will also enable organizations to persevere, despite a contested cyber environment.

> "If you are in an SEC defined critical infrastructure vertical, update your IR plans to include the mandated SEC 8K filing to be provided within 3 days of a detected event. This shortened time frame and the details that must be furnished should be considered and planned for to avoid significant fines."
>
> – Check Point CISO, Pete Nicoletti

A comprehensive incident response plan will:

- ✓ List actions and procedures for each step of the plan
- ✓ Serve the Incident Response Team and other groups
- ✓ Clarify each department's roles and responsibilities
- ✓ Explain who should escalate information to whom
- ✓ Include guidance on legally required public disclosures
- ✓ Include regulatory authority and mandatory response information
- ✓ State which metrics/evidence should be captured in relation to the incident
- ✓ Define who is responsible for what kind of business impact and analysis

ADAPT

To ensure that an organization's cybersecurity architecture evolves in tandem with the sophistication of cyber threats, organizations can leverage the following proactive, adaptive responses:

1. Implement an agile means of managing risks.
2. Apply robust analytics monitoring. Ensure that the organization assesses properties, behaviors and anomalies in an ongoing and coordinated way. Tune your systems to minimize false positives so your teams can focus on real issues, not chasing shadows.
3. Leverage contextual awareness. Consider threats and corresponding actions in the context of critical business functions and the enterprise's overall mission.
4. Ensure that security mechanisms are applied and monitored in a centralized, effective, coordinated manner.
5. Consider use of deception strategies (such as honeypots) in order to divert hackers' attention in the event that they access the network. Use Honey Tokens in your databases to alert your DLP systems for unauthorized DB access and movement.
6. Generate and use resources on an as-needed basis; for a limited time and then log-out accordingly.
7. Apply identity access management principles based on attributes of users, system elements and environmental factors.
8. Structure or restructure systems and resources to ensure alignment with organizational needs and to reduce levels of risk.
9. For critical resources, provide multiple protected instances. Use multiple backup technologies and test your restoration time frames. Think redundancy and speed to recovery.
10. Make changes to systems on a schedule that hackers wouldn't be able to guess and work around.

Organizations are also encouraged to provide education and regular updates to employees about the latest cyber security risks.

CONCLUSION

Resilience isn't just about resisting shocks and staying the same. It's really about becoming "antifragile," a concept defined within Nassim Taleb's book of the same name.

"Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better," Taleb writes.[2]

Taking a proactive approach to the resiliency framework described in this eBook will not only assist your organization in resisting and recovering from adversity, but it will also transform your organization and enable your business to become more competitive, reliable and well-regarded as a result.

After applying the best practices above, how do you know whether or not your organization is resilient?

Leverage resiliency assessment resources, such as the Cybersecurity and Infrastructure Security Agency's Cyber Resilience Review. You can also request for a vendor or expert consultant to assist with pentesting and Incident Response Preparedness workshops.

Building resilience is a continuous process that will need to evolve in tandem with your organization and the threat landscape. To ensure that your organization can recover after every adverse event, consistently advance, enrich and enhance your resilience program.

For more resilience resources, visit CyberTalk.org. Lastly, to receive more timely cyber security insights and cutting-edge analyses, please sign up for the cybertalk.org newsletter.

[2] Nassim Nicholas Taleb, Antifragile: Things That Gain from Disorder, Randomhouse. P.430