Cyber Resilience: Safeguarding the Digital Organization

Table of Contents

What You Will Learn

Cloud, mobility, Internet of Everything (IoE), and social media technologies, combined with digital business practices, have helped countless organizations transform how they operate. But they have also increased the attack surface. Old methods of cybersecurity that focus on perimeter defense are no longer enough to keep an organization safe.

Organizations recognize that cyber attacks will be launched against them. But by adopting cyber resilient architectures and business processes, they can shift from a reactive to proactive state and tackle cyber risks with confidence.

This paper:

- Defines cyber resilience
- Outlines its major benefits
- Describes the seven major system capabilities of a cyber resilient enterprise

Introduction

Today's global enterprises collect and analyze more data than ever before. They are using the information to fuel their growth, innovation, and collaboration. Cloud computing, the Internet of Everything (IoE), mobile computing, and other technological innovations are speeding the pace of change. And they're rapidly becoming a necessity for any organization that seeks to remain competitive in the interconnected global business ecosystem.

Against this backdrop of hyper connectedness and escalating online threats, every organization must be able to trust its infrastructure, its systems, and the integrity of its data. Cisco CEO Chuck Robbins has noted: "As we think about this new world, and the interwoven systems that are being created, a new level of trust is required—beyond anything in our history. We must trust the systems that manage and process the data, the people and partners who access the data, and the fundamental technologies and processes that protect the data." Chuck Robbins Cisco Blog

Even as organizations invest in and benefit from the technological advances of digitization, they are experiencing an attendant rise in cybersecurity threats. Valuable information is shared freely and frequently, and the vulnerability of that information to theft, destruction, or alteration by malicious actors continuously increases. In fact, information and security professionals know that multiple breaches could be, and most likely are, occurring in their systems right now.

Cyber resilience is the ability to prepare for and adapt to changing threat conditions while withstanding and rapidly recovering from attacks to infrastructure availability. Cyber resilience concepts provide context for implementing a risk-management strategy. Indeed, cyber resilience is largely about managing risks: identifying events that might happen, assessing how likely they are to happen and what impact they may have, and deciding what actions to take.

Questions Board Directors Should Be Asking

Board-level support is essential to cybersecurity and cyber resilience efforts. The C-suite should be able to answer these questions from the board of directors:[1]

- Have we performed a thorough assessment of our IT infrastructure?
- What is the current level of cyber risk and the potential business impact of cyber risks to our company?
- Is our cyber resilience strategy focused on our business objectives, protecting our most critical assets and revenues and providing business continuity?
- How does our cybersecurity program apply industry standards and best practices, and how does it compare with those of industry peers?
- How do we measure the effectiveness of our cybersecurity program?
- Is our cyber resilience function appropriately organized, trained, equipped, staffed, and funded?

Increasing Threat Landscapes and Risk Vectors

An organization and its board must balance the tremendous competitive advantages afforded by business digitization with the associated exposure to cybersecurity risks and costs. The average consolidated cost of a data breach in 2015 was $3.8 million, up 23 percent since 2013.[2] For companies that cannot rely on the availability of their information infrastructure in the wake of a cyber attack, costs will continue to rise in the days, weeks, and months following a breach.

Perhaps most frightening: the threat landscape is growing and changing quickly. As businesses transform into digital organizations, the threat landscape can change dramatically. For example, as companies gather, analyze, and transmit massive amounts of IoE data, their risk exposure spreads across new devices, sensors, networks, and other vectors. The technology is evolving so quickly that these devices can have multiple vulnerabilities. Likewise, the rapid integration of cloud computing, bring your own device (BYOD) policies, and mobile computing solutions increases the exposure of the information that is located on or accessed through those channels.

A common first step in enterprise digitization is the tight binding of business processing to the information infrastructure. This binding reduces operational costs and increases a business's competitive advantage. However, it also brings risks, starkly illustrated by a 2012[3] hack. A phishing attack[4] gave hackers access to a company network. After a period of preparation, malware was triggered that wiped or destroyed 35,000 disk drives across the enterprise. In a frantic effort to stem the tide of destruction, the IT staff disconnected as many devices from the network as they could. It took the company five months to return to normal business operations. During that time it conducted daily business using typewriters and fax machines on a "best effort" basis. It also bought 50,000 disk drives and hired armies of IT consultants to help clean, recover, and rebuild networks and machines. It even gave gasoline away inside Saudi Arabia after it was unable to find a way to charge for it in spite of several weeks of effort just on that one problem. In a similar situation, another company was forced to do business by hand as it struggled to keep the business going after a cyber attack in 2014.[5]

[1] Ernst & Young. Cyber Program Management. Identifying ways to get ahead of cybercrime. October 2014.
[2] IBM and the Ponemon Institute, 2015. Cost of Data Breach Study. www-03.ibm.com/security/data-breach
[3] http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676
[4] https://en.wikipedia.org/wiki/Phishing
[5] http://www.darkreading.com/sony-hackers-knew-details-of-sonys-entire-it-infrastructure-/d/d-id/1317898

As the threat landscape expands, so too does the sophistication of attacks. Data breaches by employees—whether careless or intentional—are a continuing threat, along with so-called script kiddies, amateur hackers who buy tools to perform attacks. Those continuing threats are now dwarfed by well-funded, persistent, and increasingly professional hackers, in many cases motivated and supported by nation-states. In fact, in the first half of 2015 alone, Gemalto found that 41 percent of the nearly 246 million records breached worldwide were the result of highly sophisticated, state-sponsored attacks.[6]

It should not come as a surprise then that 65 percent of the respondents to a recent Cisco Security Risk and Trustworthiness Study revealed that they believe that their organizations face a significant level of security risk.[7] The inevitability of cyber attacks, coupled with the continuing growth in criminal sophistication, pushes organizations toward cyber resilience. Cyber resilient measures can help them powerfully resist, react to, and recover from potentially catastrophic cybersecurity events within a well-defined and well-deployed risk management plan.

Developing a Digitization Strategy

The benefits of digitization are huge. By digitizing information-intensive processes, costs can be cut by up to 90 percent and turnaround times improved by several orders of magnitude.[8] Digitization creates an operating model that connects all the motions of a business—from engineering to servicing customers, and everything in between—in a synchronized and agile way. Digitization starts with making the right network infrastructure decisions. But it is just as important to reengineer an operating model to take advantage of technologies that embed process automation and analytics. Only by addressing both the technology and its labor force can an organization have a digitization strategy.

Digitization at Cisco involves:

- Simplification: Simplifying processes based on company's targeted strategic outcomes
- Automation: Automating a specific technical architecture that needs to be in place
- Monitoring and adapting: Monitoring every phase of core processes throughout the company and using analytics for machine learning in the future
- Continuous innovation: Achieving innovation through collaboration technologies

Benefits of a Cyber Resilient Architecture

The very networks and technological advances that organizations depend on for their businesses to run efficiently expose them to attacks. That is why organizations are exploring a shift from merely focusing on cybersecurity controls—which protect computers, networks, programs, and data—to cyber resilient architectures to protect their organizations and products.

If an attack penetrates a cyber resilient system within an organization, that system is able to continue to conduct mission-critical processing in a manner that preserves the confidentiality, integrity, and availability of the data. In other words, the compromised system will resist failure, and if the attack forces the system to fail, it will fail gracefully. With visibility across the network, the system can sense if it has been compromised and respond quickly. A compromised system that fails can recover to an operational state.

[6] www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx
[7] Cisco Security Risk & Trustworthiness Study. October 2015.
[8] McKinsey & Company. **Accelerating the Digitization of Business Processes**. Markovitch and Willmott. May 2014.

Cyber Resilience Goals

Cyber resilience has specific goals that focus on business preparedness, business continuity, the restoration of business functions, and business improvement:

- Maintaining a state of preparedness against attacks to prevent or reduce compromises of business functions
- Continuous monitoring to capture attack activity that cannot be blocked
- Capturing activity that is input to correlation engines that support forensics, investigation, and more sophisticated attack detection
- Continuing essential business functions despite a successful attack
- Restoring business functions to the greatest extent possible after a successful attack
- Changing business functions and cyber capabilities to reduce the adverse impacts of actual or predicted attacks

A Multidisciplinary Approach to Cyber Resilience

There are four major components of a cyber resilient IT infrastructure: people, processes, policies, and technology. First and foremost, the senior executives within the organization must provide support for the business transformation necessary to create an effective and sustainable cyber resilient infrastructure. Along with appropriate leadership from the C-level, an organization must establish processes and policies to prepare for every eventuality. The focus can then turn to selecting and implementing cyber resilient technologies to support the organization's goals and processes.

One of the many benefits of cyber resilience is that it unifies multiple disciplines, including risk assessment, technology best practices, knowledge management, risk management, and coordination of the roles of all stakeholders. The integration of cyber resilient disciplines into business practices and system architectures involves changes in the traditional ways of doing business, breaking down barriers that over time have isolated security and trust functions from mainstream management and technical processes.

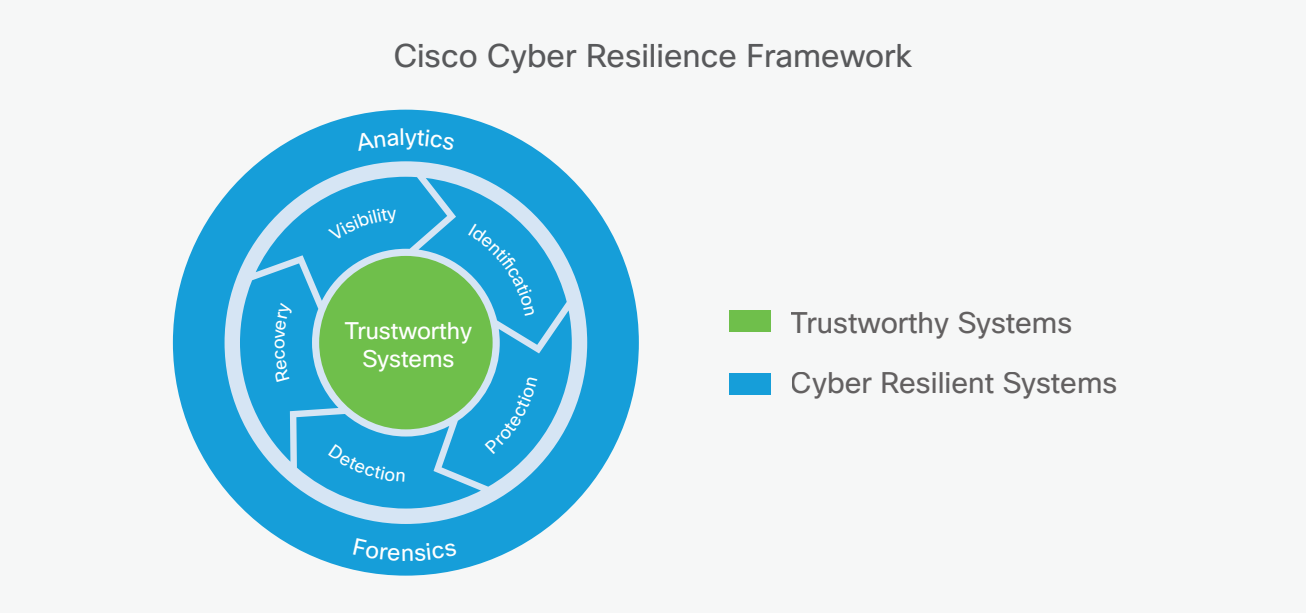
With regard to cyber resilience and cyber risk management, the higher the level of engagement by leadership and staff, the better the outcomes are likely to be.[9] As a global leader in IT, Cisco has extensive experience in engaging senior leaders in organizational transformations. We're also at the forefront of cyber resilient information and communication architectures.

An Integrated Framework

Cisco® cyber resilient IT solutions align with the guidelines and practices recommended by the National Institute of Standards and Technology, as well as with initiatives launched by the International Organization for Standardization and the World Economic Forum. For several years, Cisco has been building capabilities for providing highly secure and trustworthy foundations across our product portfolio that form the basis for a cyber resilience framework.[10]

[9] "As part of research we undertook with the World Economic Forum on cybersecurity, we had the opportunity to interview executives from more than 200 institutions and perform deep dives on cybersecurity risk-management practices with more than 60 of the world's 500 largest companies. Senior-management time and attention was identified as the single biggest driver of maturity in managing cybersecurity risks—more important than company size, sector, and resources provided." http://www.mckinsey.com/business-functions/business-technology/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

[10] Cisco Trustworthy Systems At-a-Glance. http://www.cisco.com/c/en/us/about/trust-transparency-center/built-in-security/building-trustworthy-systems.html.



Seven Capabilities of a Cyber Resilient Enterprise

Organizations continuously evaluate the trustworthiness and resilience of the systems they deploy. Understanding the foundational security concepts, principles, and best practices in support of cyber resilience goals is an essential start. In addition, an organization needs to understand how those concepts, principles, and practices can be applied to and integrated within a comprehensive systems engineering effort through cyber resilient products and solutions.

Cyber resilience is multidisciplinary and requires an organization to address multiple capabilities. The seven major capabilities that support cyber resilience goals are:

- Identification
- Protection
- Detection
- Recovery
- Visibility
- Analytics
- Forensics

Identification

The first capability in cyber resilience is identifying an organization's most valuable and critical assets. This step is crucial to making the most informed executive decisions related to both risk and investment. It's also necessary to perform an asset management and a risk assessment. To get there, an authentication capability, which ensures the confident identification of one party by another party, is essential for all systems in a network architecture.

An organization must know which devices (with specific cyber resilient capabilities) provide its cyber competencies. Only then can it maintain a cybersecurity strategy. An important aspect of tracking these devices is the Cisco Secure Unique Device Identity (SUDI), which is based on the IEEE 802.1AR standard and maintained within the Cisco Trust Anchor module. Additional aspects are the inclusion of zero-touch provisioning agents and technologies that help enable automated asset management and capability discovery.

Protection

Protection supports an organization's ability to limit or contain the impact of a cyber attack. Formally, protection is defined as the policies, processes, and mechanisms for ensuring that a system is built and operates in a state of integrity during a cyber attack or similar event, and that it is defended from modification by unauthorized or unauthenticated processes. During a cyber attack, the system can be trusted to act as designed.

To apply protection capabilities to a system, the cybersecurity engineering staff needs to identify which information or assets need protection. It must then develop an understanding of the business risks associated with those assets to prioritize the investments to protect them. This information informs decisions about the level of effort (and therefore cost) appropriate to protect the system and the data it processes. Cisco's Security and Trust Organization has developed trustworthy mechanisms to support protection.

Detection

Detection is defined as the policies, processes, and mechanisms to measure, collect, verify, and analyze system integrity. The detection mechanism may be enhanced through the use of an additional verifier, analysis module, and forensics for a more robust system. Cybersecurity engineering develops and implements the appropriate mechanisms to identify the occurrence of a cyber attack. Detection enables the timely discovery of it.

The detection mechanism works closely with visibility to ensure notifications of behavior. It logs and forwards events when an unexpected behavior is identified. Detection is an area of special current attention within security and trust organizations. Cisco is developing general detection requirements for features that will detect malware or tampering of its software products.

Recovery

Recovery is defined as the policies, processes, and mechanisms for restoring a system to a state of integrity. Recovery is a fundamental distinction between cybersecurity and cyber resilient systems, and it supports the timely recovery to normal operations to reduce the impact of a cyber attack.

The goal of a recoverable system is to restore the normal operation of a platform, application, or service if it becomes corrupted through a cyber attack or misconfiguration. Recovery can be accomplished through new platform capabilities that allow a recovery agent to run and correct or replace the compromised system components, including firmware, applications, user data, configuration data, and software.

Recoverable systems provide either local protected storage to safeguard recovery agents from tampering by malware, or a reliable and highly secure means to download recovery agents from a source over a network. Recoverable systems greatly reduce costs and downtime when a cyber attack occurs. A platform can be recovered to any of the following appropriate states:

- Reset to factory defaults
- Update to the newest firmware image
- Restore to a last known good configuration
- Perform a partial "repair" operation
- Recover to an enterprise-defined "starting point" or gold standard
- Apply an architecture modification to account for a gap
- Any combination of the above

Visibility

Visibility provides continuous awareness to an external entity of the system's state of integrity. Protection, detection, recovery, analytics, and forensics are all supported by a visibility mechanism.

The tools for visibility are typically integrated with cyber resilient protection, detection, recovery, analytics, and forensics capabilities to establish a coordinated security and compliance posture that can provide the state of integrity of the system to administrators, users, tools, applications, or third parties.

Visibility enables supports the continuous monitoring and tracking of the state of integrity of an organization's assets. It also provides a method for each device's detection mechanisms to communicate to the organization's forensics. These assets include:

- Application security
- Audit and compliance
- Business continuity and operations
- Change control and configuration management
- Data and data center security
- Governance and risk management

- Identity and access management
- Infrastructure and virtualization security
- Security incident management, e-discovery, and cloud forensics
- Supply chain management
- Threat and vulnerability management
- Location

Analytics

Analytics gathers and examines cyber attacks to bring situational awareness and to help IT staff identify events that pose the greatest risk. Analytics is one of the most effective defenses against cyber attacks. It reduces the critical time from detection to recovery, so that cyber specialists can proactively defend your network.

Forensics

The seventh capability is forensics, defined as the processes and specialized techniques for ingesting relevant support data, along with preserving, processing, analyzing, and presenting system-related evidence in support of recovery.

The large number of security incidents affecting many organizations and the increasing sophistication of cyber attacks are the driving forces behind digital forensics. Machine learning and manual analysis are used to examine historical information and to search for anomalous events (reverse engineering).

Conclusion

Digitization provides organizations with opportunities to grow and innovate. But it also brings a new world of risks, especially to one of an organization's most valuable assets—its information. That information is crucial to the future success of an organization and is likely valued by a wide range of adversaries. With the rapid adoption of digitization, it's easier than ever to target and attack that information. Applying cyber resilience capabilities and state-of-the-art security across the enterprise will allow an organization to tackle its cyber risks with greater success.

Transforming into a cyber resilient organization requires a detailed roadmap that specifies how the organization must develop and implement a cyber resilient IT infrastructure. Also paramount is having a knowledgeable partner with established cyber resilience practices, extensive experience, and a proven commitment.

The seven capabilities of cyber resilience will not completely eliminate the possibility of a breach. However, implementing them will provide a highly effective defensive posture that meets the expected standard of a comprehensive assessment of an organization's risks to cyber attacks.

As a security and architectural leader in cyber resilience, Cisco is fully committed to the continual innovation, research, and development of cyber resilient solutions to protect customers, their networks, and their businesses. We provide our customers with cyber resilient information, communications systems, and the capability to verify that our platforms and software, used to build our own IT infrastructures, are cyber resilient.

For More Information

To get started on the journey toward cyber resilience, visit Cisco's Trust and Transparency Center.

C11-736966-00 03/16