July 2016

Cyber resilience – going beyond security to a new level of readiness

An article by Mike Del Giudice, CISSP, CRISC, and Chris Wilkinson, CISSP, CRISC

Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

In recent years, the term “cyber resilience” has become increasingly common in discussions about cybersecurity, risk management, and related issues.

At first glance, this might appear to be just another case of “cyber” overload – the attachment of the prefix to various words to produce trendy-sounding catchphrases such as “cyber threat,” “cyber hygiene,” “cyber trespassing,” and even (to cite one government official) “cyber Armageddon.”

In fact, cyber resilience is more than just another buzzword. It describes a different and useful way of thinking about protecting data and information systems. Rather than focusing only on preventing attacks or intrusions, cyber resilience also focuses on mitigating the consequences of such incidents.

As attacks on data and information systems become increasingly prevalent – and increasingly malicious – the concept of cyber resilience can help organizations of all types and sizes do a better job of minimizing the damage caused by these attacks.

Today’s threat environment

Cybersecurity has been a serious concern in both the public and private sectors for quite some time, but the level of concern has increased in recent years as new types of threats have emerged. Among the most pervasive of the current generation of threats are ransomware (malicious software that blocks access to a system or data until a sum of money is paid) and whaling (targeted scam emails that appear to be from a high-level executive or other legitimate authority).

Threats such as these are not only more difficult to detect than earlier types of incidents but also more malicious in their intent and more devastating in their potential effects. Their consequences are often immediate and severely damaging.

For example, the newest types of ransomware no longer merely hold a company’s data hostage until a ransom is paid; they actually start destroying data if the ransom isn’t paid quickly.[1] Another recent – and particularly alarming – ransomware trend has been the high-profile targeting of numerous hospitals and other healthcare facilities,[2] which scammers view as being more likely to pay a ransom because blocking critical data directly affects patient outcomes and could cost lives.

Moreover, all signs point to attackers continuing to grow more devious and demanding. Witness, for example, the recent experiences of one prominent hospital that opted to pay a ransom rather than risk patient outcomes, only to encounter a repeat ransomware incident a few months later when the perpetrators returned for a second helping.

Not whether but when

Today's threat environment differs from that of years gone by in another important way. Most security experts have come to recognize that, as attackers become more numerous, persistent, and cunning, prevention alone is no longer an adequate strategy. Most organizations of any appreciable size long ago came to grips with the idea that intrusion attempts are virtually inevitable. Today, though, the same organizations are also recognizing the near certainty that some of these attempts will succeed.

In other words, it's no longer a question of whether an attack will succeed, but when. And that raises the more important question: What steps can an organization take to minimize the effects of the attack?

That outlook is the underlying mindset that drives organizations to begin embracing cyber resilience – a concept that draws together various practices related to security, disaster recovery, and business continuity. Until recently, these disciplines have been viewed as related but distinct from each other.

However, cyber resilience integrates principles and practices from all these fields into a comprehensive readiness and response effort that encompasses three broad phases:

1. **Incident management** – The immediate response to an attack, designed to limit the damage and prevent it from spreading
2. **Service continuity management** – Processes that allow the organization to continue operating, performing only its most essential functions in a diminished capacity, in the immediate aftermath of an attack
3. **Disaster recovery** – Processes and practices designed to help the organization get back to normal and resume full operations as quickly as possible

Cyber resilience models and related standards

Much of the thinking behind cyber resilience can be traced back to work done for the United States Computer Emergency Response Team (US-CERT), a division of the U.S. Department of Homeland Security. Working with Carnegie Mellon University's Software Engineering Institute, the team created the CERT Resilience Management Model (CERT-RMM) in 2010, to converge various risk management activities – such as security, business continuity, and IT operations – into a single model.

The department's website describes the model as a "process improvement approach" that can help organizations "respond to stress with mature and predictable performance." A year later, US-CERT produced the Cyber Resilience Review (CRR), a "voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices."

Although developed separately, the CERT-RMM and the CRR align closely with the central tenets of the widely used National Institute of Standards and Technology (NIST) cybersecurity framework, which many industries have adopted. The CRR enables an organization to relate its cyber resilience capabilities to the NIST framework, using a document, which some call a "crosswalk," to compare the two approaches and map the features they have in common.

Many industries have adopted the NIST cybersecurity framework, and both the CERT Resilience Management Model and the Cyber Resilience Review align closely with its central tenets.

Components of cyber resilience

As updated in 2016, the CERT-RMM organizes cyber resilience into 26 separate process areas, ranging from “ADM: Asset Definition and Management” to “VAR: Vulnerability Analysis and Resolution.” The CRR condenses these areas into 10 domains:

1. **Asset management.** Asset management establishes an organization’s inventory of high-value assets in four broad categories – people, information, technology, and facilities – and defines how these assets are managed to support the organization’s critical services. The purpose is to identify appropriate strategies that will allow these assets to remain productive during disruptive events.
2. **Controls management.** Controls management involves identifying, implementing, and assessing the administrative, technical, and physical controls that are used to maintain mission-critical services and assets. This effort applies both to operational controls, which are implemented by the organization’s operating units, and to enterprise controls, which apply universally across the entire organization.
3. **Configuration and change management.** As the complexity of information systems increases, the complexity of the processes used to create them also increases, as does the probability of configuration errors. Configuration and change management is a continuous process of controlling and approving changes to information or technology assets or changes to related infrastructure.
4. **Vulnerability management.** A vulnerability is any physical or operational feature that could make the organization susceptible to risk from a natural event or manmade threat. Vulnerability management focuses on the processes used to identify, analyze, and address such vulnerabilities, particularly those weaknesses that would affect a critical service of the organization.
5. **Incident management.** Some disruptive events are relatively minor. Others, however, such as natural disasters, loss of a primary data center, or a cyber attack that disrupts critical infrastructure or services, can require the entire organization to mobilize resources. The goal of incident management is to improve the processes that are used to detect, identify, evaluate, and respond to disruptive events.

6. **Service continuity management.** Service continuity planning spells out predefined procedures for sustaining essential operations in varying adverse conditions, ranging from minor interruptions to large-scale incidents, regardless of their cause. Beyond planning, service continuity management identifies the services that are most important to carrying out the organization’s mission as well as the design, development, validation, and testing of response plans.
7. **Risk management.** Risk management, a foundational activity for any organization, is practiced at all levels. In the context of cyber resilience, risk management refers to processes that identify and analyze the operational risk of IT-dependent assets and services. Risk management also encompasses the determination of how to deal with (avoid, accept, transfer, or mitigate) those risks in ways that reflect the organization’s tolerance for risk.
8. **External dependency management.** Most organizations rely on a variety of outside entities, including technology vendors, raw material suppliers, public infrastructure, and other services. The management of external dependencies focuses on establishing appropriate controls to protect assets and sustain critical activities that depend on these relationships.
9. **Training and awareness.** The training and awareness domain focuses on seeing that staff members have the knowledge and skills they need to perform their work in incident management, controls management, risk management, and other related domains. It also involves making staff members more aware of their roles in the cyber resilience effort.
10. **Situational awareness.** Situational awareness means providing stakeholders with accurate and up-to-date information about the immediate operational condition of critical services so that they can make decisions effectively. It also involves coordinating this information through timely communication to appropriate decision-makers.

These 10 domains provide a helpful framework for understanding the concept of cyber resilience. In addition, they provide organizations with a structure useful for organizing their cyber resilience efforts. When related to either the NIST or a comparable framework, these 10 domains can help risk managers and other responsible parties plan how best to deploy various assets – including people, information, technology, and facilities – in support of specific operational missions or critical services.

Moving beyond effectiveness to maturity

As noted earlier, US-CERT produced the CRR in order to provide a voluntary, nontechnical assessment that organizations could use to measure and evaluate their operational resilience in the face of various types of disruptive events. It is important, however, to avoid the natural tendency to regard the review as a checklist or compliance standard.

Rather than approaching cyber resilience from a compliance mindset, a more useful approach is to use such assessments as a way to advance an organization's cyber resilience toward a higher maturity level. The difference is more than just a matter of semantics.

A checklist suggests that the organization either meets or fails to meet a certain standard. Its efforts are either effective or ineffective. Maturity, on the other hand, encompasses not only effectiveness but also two additional important attributes: efficiency and responsiveness.

Say, for example, that an organization establishes a series of manual activities that must be performed as part of its patch management protocol. Such a manual arrangement might be perfectly acceptable and deemed effective, but it does not necessarily reflect a high level of maturity. A more mature organization might choose to automate those same processes in order to go beyond effectiveness to become more efficient or reduce opportunities for errors or oversights as well as become more responsive to change.

Implementing a cybersecurity resilience program

As with all cyber-based programs, the risk and threat landscape is broad and continually maturing, often at a quicker pace than the internal responses to those threats. The most effective approach to managing such risks is to start with a comprehensive risk assessment in order to identify which areas to address to provide the most value to the organization.

The risk assessment will identify the cyber resilience components that would be the most advantageous for the organization to address in the short term, while also providing a general road map for the organization as the program matures. For example, organizations with little reliance on third parties would see less value in focusing on external dependency management than would a company that has outsourced critical business systems.

Absent a risk assessment, organizations should focus on the following critical components in the short term:

1. **Incident management.** Cyber resilience is based on the concept that a breach will happen eventually, and the ability to respond to an incident effectively is a critical component of any resilience program. Organizations should proactively identify a formal program and response team. To improve the program's efficacy, it should include training and testing exercises.

2. **Vulnerability management.** Organizations must have visibility into the vulnerabilities in the existing environment in order to manage them appropriately. The ability to mitigate these vulnerabilities, whether through available system patches or other mitigating techniques, greatly decreases the likelihood of an incident becoming a breach.
3. **Training and awareness.** The weakest point of any security effort is typically the end user, which is why phishing continues to be a threat that has led to some of the most widely publicized breaches. Most organizations have training programs, but they must determine if these programs actually increase awareness or just "check the box."
4. **Controls management.** Controls management is a broad topic that requires constant attention. Initially, however, the focus should be on managing those risks related to advanced endpoint protection.

   In reality, managing employee behavior in the face of very advanced phishing schemes is difficult, and even with critical training, incidents will still occur. Organizations need to evaluate technical controls at the endpoints to minimize the impact of an incident when it does occur.

More than compliance

By approaching cyber resilience from the perspective of maturity, rather than just effectiveness, an organization can help make cyber resilience efforts more than exercises in compliance. With the establishment of a foundation for improved decision-making, it can even develop cyber resilience beyond its primary function as an important risk management tool. A cyber resilience program can limit an incident's impact, increase business continuity, and hasten recovery – ultimately adding value to any organization.

Learn more

Mike Del Giudice is with Crowe and can be reached at +1 630 575 4359 or mike.delgiudice@crowe.com.

Chris Wilkinson is a principal with Crowe and can be reached at +1 219 308 8980 or christopher.wilkinson@crowe.com.

[1] Lawrence Abrams, "Jigsaw ransomware decrypted: Will delete your files until you pay the ransom," bleepingcomputer.com, April 11, 2016, http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/

[2] Kim Zetter, "Why hospitals are the perfect targets for ransomware," Wired, March 30, 2016, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

crowe.com

Text created in and current as of July 2016; Cover and artwork updated in May 2018.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.