Cyber resilience

Protecting companies from cyber-triggered business disasters

EY
Building a better working world

We live in a world in which data breaches and destructive cyber attacks have become a daily headline. By now, everyone has received a breach notification letter or an email apology from a company impacted by a major cybersecurity issue. Boards are asking, customers are asking, and the employees are asking, the whole world seems to be asking one simple question:

Why?

The old talk track

The short answer is: there are a lot of reasons. In fact, the commonly accepted narrative explaining why has almost become a cliché.

> **The volume and sophistication of cyber attacks have increased, while companies' ability to defend against the attacks has decreased. Security budgets are insufficient, and the talent pool for cybersecurity professionals is in a deficit. It's not a matter of if we will be hacked, it's when. And in all likelihood, we are being breached right now and don't even know it.**

Sound familiar?

This talk track is repeatedly recited by chief information security officers and chief information officers, and is usually:

- Followed by a security framework, assessment and benchmark that
- Aligns to industry-leading practices and standards, and is
- Accompanied by a huge budget request for a portfolio of roadmap initiatives that will save the company from impending doom

This pattern of pitching cybersecurity is normal — and even necessary — for most companies seeking to stay competitive and secure in a digital world. In fact, recently boards have been asking, **"Are we doing enough?"** In most cases, the answer is clear: **no.** But it is a difficult question to definitively answer with any level of specificity. After all, how much security is ever enough? Like all investments, establishing the "right" level of cybersecurity is a constant balance between value, cost and risk. Perhaps a better question to ask is:

> **"What are we doing to make sure we can bounce back quickly when our company is attacked?"**

In other words:

> **Are we resilient to cyber attacks?**

A new definition

Cyber resilience is defined as **an organization's ability to prepare for, respond to and recover from cyber-triggered business disasters.** This definition has a few key components:

The proactive steps an organization takes to ready itself for an adverse event

The reactionary measures implemented to counter the impacts of an adverse event

Restoration of service during and after an adverse event

The last critical component is the idea of a cyber-triggered business disaster (synonymous with "adverse event" in the component descriptions).

In recent years, cyber attacks have shifted from experimentation, fraud, extortion, blackmail and data exfiltration to more damaging impacts, such as system destruction, data eradication and data manipulation. The Petya and NotPetya malware showed the world how quickly computer viruses can spread and how damaging they can be to a company's business operations and, ultimately, its core mission. The damages caused by NotPetya reached an estimated $10b, exceeding the $4b–$8b estimated losses[1] caused by the WannaCry outbreak one month earlier. That is why we have shifted away from labeling these events "incidents," "cyber attacks," or "hacks" – that does not capture the severity of their impact on business. We must recognize that these events are really an existential attack on the business itself that can have disastrous effects, fundamentally threatening the going concern of a company.

1 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Today's resiliency function

There are many debates about what constitutes an effective and holistic set of resiliency functions, but there are four commonly accepted disciplines within a company that have come to be associated with **"resilience."**

Security incident response (SIR)

Security incident response, or SIR,[2] typically exists within any high-performing security operations center (SOC). As events are logged, correlated and analyzed, SOC analysts escalate suspicious activity for investigation. Events may turn into security incidents, which are formally dealt with by trained responders. It is critical to have an effective SIR program in place, as seemingly insignificant events may quickly escalate to massive breaches and have destructive consequences for a company. SOC analysts and security incident responders are the frontline troops in the battle against malware and hackers.

2 SIR is sometimes referred to by security professionals as "incident response" or IR, which is different from general IT incident response. For the purposes of this article, we are differentiating SIR as the function that exists within the security organization to respond to and address qualified cybersecurity incidents.

Business continuity management (BCM)

Business continuity focuses on keeping the business operating. It is the process of developing and documenting arrangements and procedures that enable the organization to respond to an event that lasts for an unacceptable period of time and to resume critical functions after an interruption. Effective BCM results in the creation and practice of a business continuity plan, which outlines a company's critical business processes, and designs plans for overcoming adverse events (such as natural disasters, epidemics, supply chain disruptions and potential geopolitical risks, just to name a few). While BCM may sound similar to cyber resilience, BCM's mission includes a wider array of business disruptions. By contrast, cyber resilience is acutely focused on cyber-triggered business disasters. High-impact cybersecurity events have become an ever-growing chapter in the book of business continuity plans, and what was once a chapter now deserves a book itself.

Disaster recovery (DR)

Disaster recovery focuses on restoring the technical infrastructure in the event of a disaster. It is the technical (e.g., application, network, platform and storage) component of business continuity management to recover a data center, service or application. DR can be at odds with security incident response functions. While DR personnel's objective is high availability and their mission is to restore service as quickly and seamlessly as possible, security incident responders care more about threats to systems and data confidentiality and integrity. Though restoring system availability is critical, security incident responders work to understand the root cause and source of the attack in order to implement the appropriate countermeasures, which can include quarantining and isolating portions of the network or infected systems.

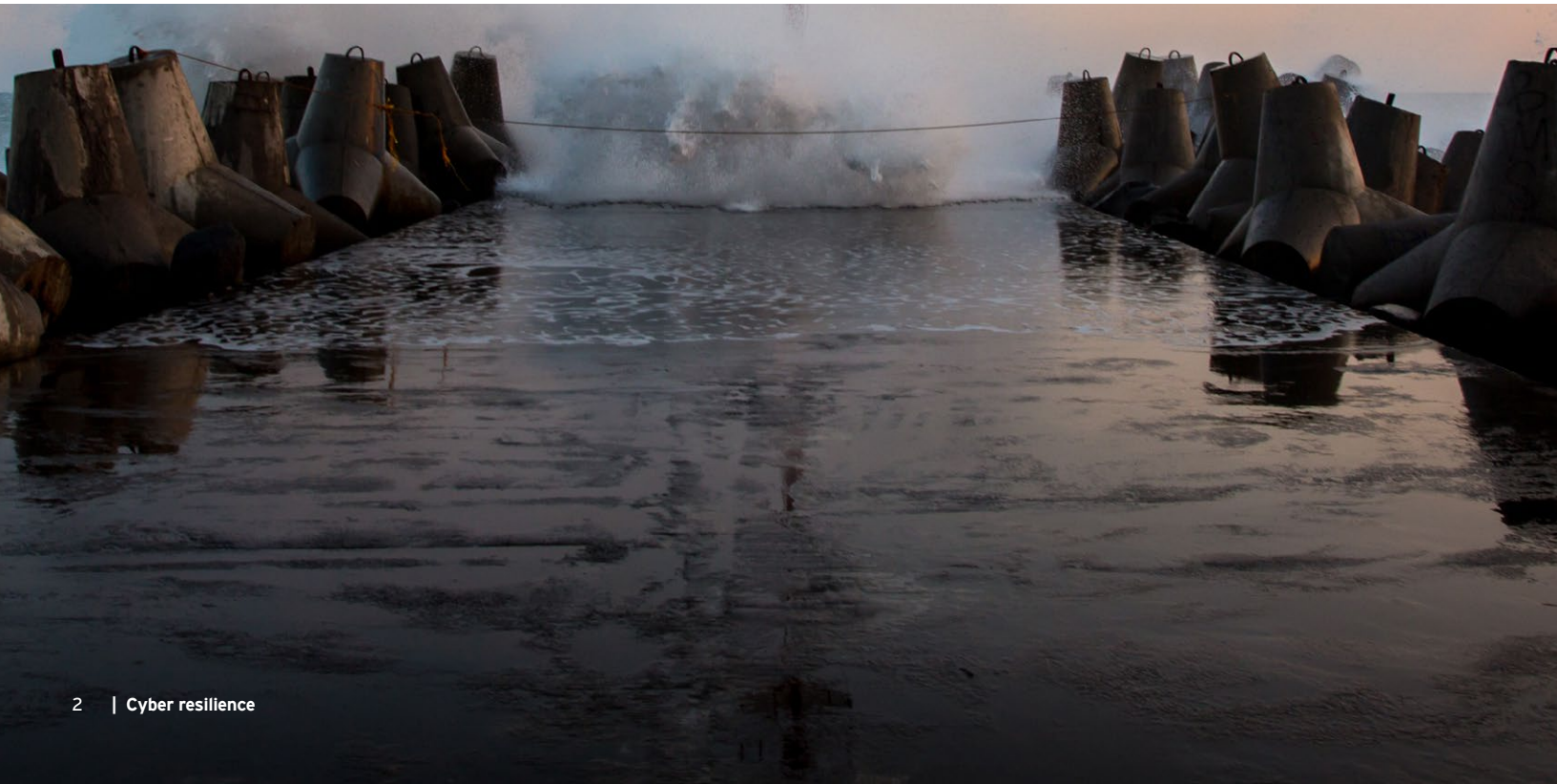
Crisis management (CM)

Crisis management focuses on responding to extreme disruptions that threaten the financial, operational or reputational assets of a company. It is a coordinated plan of responding to, and managing through, damaging events. Crisis management helps companies respond to widespread, rapidly escalating, high-impact events not traditionally covered by BCM.

There are also a number of supporting functions that contribute to a company's resilience agenda, such as enterprise risk management, internal audit, legal, public relations (when a crisis occurs), and fraud and investigations. While the capabilities above are described in silos, more advanced companies are fusing together resilience-related functions across the multiple "lines of defense." This convergence has helped organizations move from detective to **preventive** and from reactionary to **predictive,** but it takes a significant and deliberate effort to achieve this level of maturity.

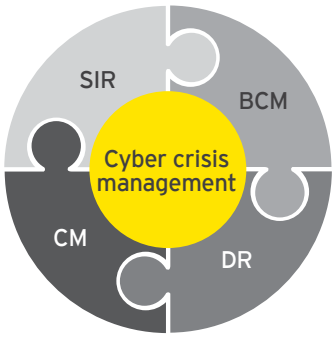
Until recently, meaningful integration between resilience functions was difficult, to the point of being impossible, in large organizations. Advances in technology (e.g., artificial intelligence and machine learning), system monitoring and sensors, analytics and reporting, and platform integrations and APIs have enabled us to bring data together faster to make smarter decisions with less effort.

Yet, even as the people, processes and technology supporting these resilience functions are converging, there still remains a missing critical piece of the puzzle, and its absence continues to be one of the leading reasons why companies fail to effectively respond to cyber-triggered business disasters.



The missing piece

The SIR-BCM-DR-CM model has remained relatively unchanged since their respective disciplines were formalized into corporate functions. Yet, there is a missing piece in this model, a function that is absent from many companies and is one of the leading (but not only) contributing factors in the sharp increase in cyber-triggered business disasters.



It is the discipline of cyber **crisis management.**

This discipline is the missing link between SIR and BCM. It serves as the coordinating function when a cyber-triggered business disaster occurs that exceeds the severity, impact, duration or organizational reach of traditional SIR functions. It allows SOC operators and security incident responders to focus on defending against attacks while yielding command and control and, perhaps most importantly, the coordination responsibilities to another organization empowered to resolve the end-to-end cyber crisis.

Many SOCs do a fine job of triaging security incidents that arise in the daily course of monitoring the corporate environment. However, when large-scale cyber attacks occur that result in the loss of critical business services — and require coordination of many corporate functions — the SOC does not perform well in resolving the problem. Nor should they. It is beyond their remit for two reasons: skill and scale.

On the skill front, to use a medical analogy, it's like asking your family doctor to perform heart bypass surgery. Though he or she may be a doctor, one needs a specialist with a different set of skills to ensure a more successful outcome. Likewise, the complex resolution of a cyber-triggered business disaster also requires specialists with a different set of skills.

Continuing with the medical analogy, on the scale aspect, it is akin to one's local emergency room (ER) handling a widespread outbreak of Ebola. Though the frontline responding organization may initially be the ER, it won't be long before the epidemic is escalated to the Centers for Disease Control for additional resources with a broad reach to manage and quarantine the major health crisis. Cyber-triggered business disasters operate at a scale of epidemic proportions, yet we often respond to them like they are ordinary visits to the ER.

Traditionally, large-scale cyber attacks may have resulted in activation of a contingency plan described in the business continuity plan. The issue with this is that cyber attacks are unpredictable, indicators of compromise trickle in, and many business continuity plans inadequately address the nuances and complex scenarios of a major cyber attack. To make matters worse, BCM, as a corporate function, is often composed of part-time volunteer resources. Companies rarely dedicate resources to the BCM function as a stand-alone entity, so when disaster strikes, it's an all-hands-on-deck call to action of volunteer "firefighters."

By the time a large-scale cyber attack or destructive malware has spread throughout the environment, it may be too late for DR

procedures because the backups may have been rendered useless or inaccessible. This is usually when a cyber-triggered disaster turns into an all-out company crisis. While crisis management functions are used to dealing with corporate reputational issues, they lack the technical knowledge and command-and-control capabilities necessary to maintain calm while simultaneously restoring service and keeping the right stakeholders informed.

With the rise of destructive attacks and malware, we can now see why this new function, cyber crisis management, is a missing piece of the solution that companies must consider as part of their overall resiliency program in order to achieve true cyber resilience.

The cyber crisis command center (C4)

In this new model, the cyber crisis management function begins where the security incident response function ends. Rather than trying to triage a problem that is too big to manage, the SIR team moves the incident to the cyber crisis command center (CCCC, or C4 for short). The C4 is in charge of sensing and detecting, responding to, recovering from and adapting the organization's capabilities to better respond to large-scale cyber attacks. Specifically, the C4 focuses on:

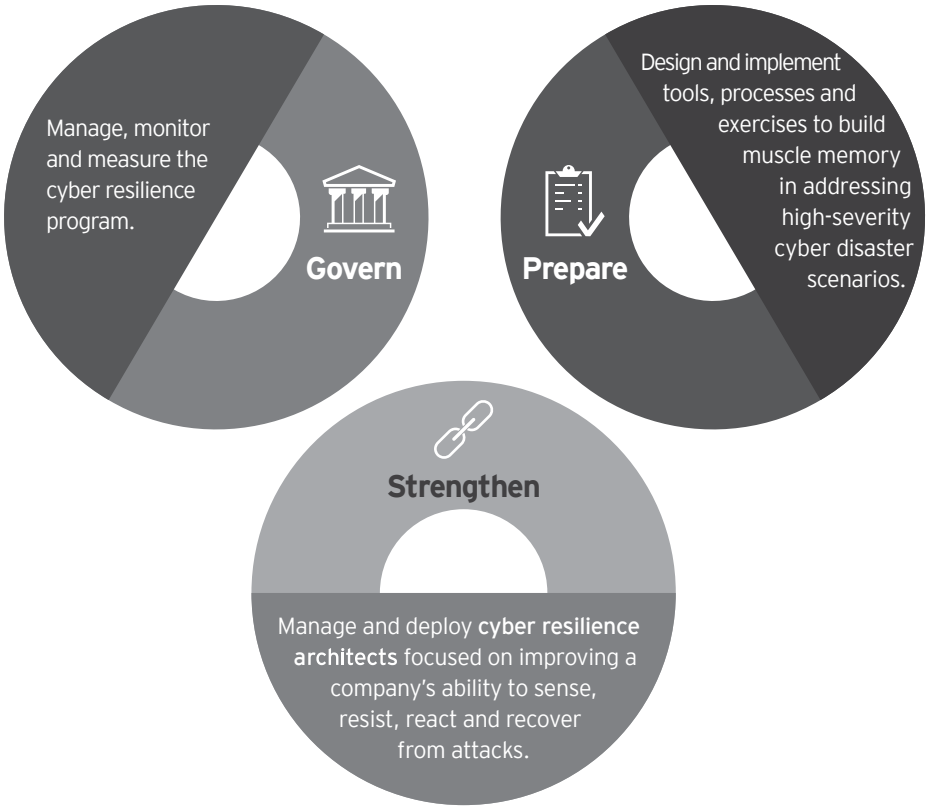
- Monitoring channels for indicators of compromise. This is not meant to replace the SOC function; rather, it complements the security monitoring and detection metrics portfolio. Channels can include social media, DLP (data loss prevention and protection escalations), network traffic and CPU spikes, and malware propagation metrics. The key is to embed "sensors" into various sources of leading indicators of escalating cyber attacks.
- Establishing command and control during a cyber crisis.
- Convening and coordinating the disparate functions at the right time (such as PR, IR, DR, legal, network operations, business stakeholders, and external partners and vendors).
- Evaluating and deciding on potential courses of action toward resolution.
- Controlling the messaging and flow of information related to the disaster.
- Informing and involving the C-suite and board at the right time with the right information.
- Coordinating restoration of service while preserving evidence and investigating the root cause.
- Remediating short-term root cause issues to prevent the attack from occurring again. Whether applying patches, shutting down open ports or blocking suspect IP addresses, the C4 would coordinate the resistance countermeasures with the SOC and investigate and recommend longer-term solutions for proactive remediation. (Note: longer-term remediation activities would likely be carried out by other departments but would involve cyber resilience architects [described in the next section] in the design, build and deployment of the solution.)

The C4 will inevitably take on more responsibilities, but fundamentally it brings the right people together to make the right decisions at the right time based on the right information. It cuts through the red tape of company bureaucracy during a cyber crisis while making certain that its actions align to a set of principles, such as preserving evidence, prioritizing customer and stakeholder interests, and ensuring legal compliance.

Proactive cyber resilience

While cyber crisis management is a vital component of an effective cyber resilience program, it only solves for the reactive part of the resiliency equation. Establishing a cyber resilient company also means launching proactive measures to design and build systems that are "resilient by design" from the very beginning.

To address this, a cyber resilience program should have three proactive functions to complement the reactive cyber crisis management capability.



These proactive functions work hand in hand with the reactive functions of a cyber resilience program.

As new cyber crises are discovered and resolved, new solutions, enhanced processes and stronger controls are designed by resilience architects so they may be implemented across the enterprise environment. Cyber resilience architects design and build architectural resiliency patterns that are implemented and evangelized throughout the company. The goal of the resilience architecture function is to embed the right security controls into the environment from the beginning. For legacy systems that cannot implement sufficient levels of security controls, cyber resilience architects act as advisors to help design and implement reusable mitigating solutions and help business stakeholders craft plans for modernization to secure and trusted platforms. By operating a cyber resilience capability with these proactive and reactive aspects, a company will be better able to overcome the rising threats of cyber-triggered business disasters.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

1810-2940138

ED None

ey.com

This article was written by Justin Greis (justin.greis@ey.com) and first appeared on progressology.com. It has been edited and reprinted with the author's permission.