Cyber resilience: protecting companies from cyber-triggered business disasters

We live in a world where 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 *cyber bad guys.* Boards are asking, customers are asking, employees are asking, the whole world seems to be asking one simple question: "*why?"*

The old talk track

I'm not going to kid you: 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 has increased while companies' ability to defend against the attacks has decreased. Security budgets are insufficient and the talent pool for cybersecurity professionals is in 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 naturally recited by CISOs and CIOs, and is usually:

…followed by a security framework, assessment, and benchmark, which…

…aligns to industry leading practices and standards, and is…

…accompanied by a huge budget request for a portfolio of roadmap initiatives which will save the company from impending doom.

Don't get me wrong, this pattern for 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:

- *Preparation* – the proactive steps an organization takes to ready itself for an adverse event.

- *Response* – the reactionary measures implemented to counter the impacts of an adverse event.
- *Recovery* – restoring service during and after an adverse event.

The last critical component is the idea of a c*yber-triggered business disaster* [synonymous with "adverse event" terminology above].

In recent years we have seen cyber attacks shift 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 core mission and operations. The damages caused by *NotPetya* reached an estimated $10 billion, exceeding the **$4-8 billion estimated losses** caused by the *WannaCry* outbreak one month earlier. That is why we have shifted away from labeling these events "incidents, cyberattacks, or hacks" – that does not capture the severity of their impact on the business. We must recognize that these events are really an attack on the business itself and they can have disastrous effects that fundamentally threaten the going concern of a company.

Today's resiliency function

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

1. Security incident response (SIR)

Security incident response (or "SIR" and sometimes called incident response or "IR." For the purposes of this article we are differentiating SIR from general IT incident response) 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. 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 events and scenarios (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. I believe that 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.

3. Disaster recovery (DR)

Disaster recovery focuses on getting the technical infrastructure up and running in the event of a disaster. It is the technical (e.g. application, network, platform, and storage) component of business continuity planning to recover a data center, service, or application. Disaster recovery 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 system/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.

4. 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 (ERM), Internal Audit (IA), Legal, Public Relations (PR) [when crisis hits], and Fraud/Investigations. While I described the capabilities above 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 significant and deliberate effort to get there.

Until recently, this level of 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/sensors, analytics and reporting, and platform integrations/APIs have enabled us to bring together data 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 critically missing piece of the puzzle that I believe is one of the biggest culprits for companies failing to effectively respond to cyber-triggered business disasters.

The missing piece

The S*IR-BCM-DR-CM* model has remained relatively unchanged since their respective disciplines were formalized into corporate functions. Yet I believe there is a critically missing piece in this model; a function

that is absent from many companies and is one of the biggest (but not only) contributing factors to the sharp increase in cyber-triggered business disasters.

It is the discipline of *Cyber Crisis Management*.

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

Many security operations centers 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 loss of critical business services – and require coordination of many corporate functions – the SOC does not perform well in resolving the problem. And 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 bypass heart 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, a cyber-triggered business disaster also requires specialists with a different set of skills.

Sticking 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 front-line physicians may initially be the ER, it won't be long before the epidemic is escalated to the Center of Disease Control (CDC) 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 ordinary visits to the ER.

Integrating cyber crisis management

Traditionally, large-scale cyberattacks may have resulted in activation of a contingency plan or scenario described in the business continuity plan. The issue with this is: cyber attacks are unpredictable, indicators of compromise trickle in, many business continuity plans inadequately address the nuances and complex scenarios of a major cyber attack. To make matters worse, business continuity management, as a corporate function, is often composed of part-time volunteer resources. Companies rarely dedicate resources to the BCM function as a standalone 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 Disaster Recovery plans because the backups could 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 cybersecurity 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 would move 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 large-scale cyber attacks. Specifically, C4 focuses on:

- Monitoring channels for indicators of compromise. This is not meant to replace the SOC function; rather, complement the security monitoring and detection metrics portfolio. Channels can include social media, DLP (data loss prevention/protection escalations), network traffic/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 crises.
- Convening and coordinating the disparate functions at the right time (such as PR, Incident Response, DR, legal, network operations, business stakeholders, external partners, etc.).
- Evaluating and deciding on potential courses of action towards 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 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/recommend longer-term solutions for proactive remediation. (Note: longer-term remediation activities would be carried out by other departments but would involve Cyber Resilience Architects [described in next section] to ensure solutions are implemented and applied enterprise-wide.)

The C4 will inevitably have more responsibilities added to its scope, 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 while ensuring its actions align to a set of principles such as preserving evidence, prioritizing customer and stakeholders 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 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:

- *Govern* – manage, monitor and measure the cyber resilience program.
- *Prepare* – design and implement tools, processes, and exercises to build muscle memory in addressing high-severity cyber disaster scenarios.
- *Strengthen* – manage and deploy *Cyber Resilience Architects* focused on improving a company's ability to sense, resist, react, and recover from attacks.

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 fed to the architects so they may activate and implement those measures in the environment. We believe that, 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.

What are you seeing?

It is our observation that most companies:

1. do not have a dedicated Cyber Crisis Management function or a C4 organization, and they
2. do not have a dedicated set of security architects focused on making the organization more resilient against cyber-triggered business disasters.

Rather, they rely on security incident response capabilities or part-time BCM, DR or Crisis Management stakeholders.

Credits

- This article includes significant contributions and edits from **Heather Gantt-Evans**, **Kevin Eiden**, and **Chad Elkins**.
- Special thanks to **Dan Stavola** for his review and insights on drafts of this article.

justin greis

hi, i'm justin

(nice to meet you)

I post weekly **professional insights** and **personal stories** from my life as a management consultant, a dad, and an eternal optimist.

Click here to learn more about my **professional**, **personal**, and **"perfessional"** background.

connect with me

- **Visit JustinGreis.com**
- **Learn more about Justin**
- **Subscribe to newsletter**
- **Contact Justin**