DATA GUARD

The CIO's Guide to

CYBER RESILIENCY

* * * *

UNDERSTANDING CYBER-RESILIENCE

Your organization may have a robust cybersecurity toolbox, but security tools alone do not amount to a strong cyber-resilient posture. Understanding how cyber-resilience and cybersecurity are uniquely different yet complementary is fundamental to achieving your desired outcomes. As Chief Information Officer (CIO), you are painfully aware that the odds of a successful cyber-attack on your organization are not in your favor. Questioning if you'll eventually fall victim to cybercrime will always be answered with a resounding "Yes." By adopting a solid stance of cyber-resiliency, your organization will be better equipped to ensure Business Continuity in the face of cybercrime..

- Cybersecurity refers to leveraging methods, processes, and tools to protect data, networks, and devices from criminal use or unauthorized access and ultimately ensuring business operations, assets, and resources' confidentiality, integrity, and availability (CIA). Cybersecurity aims to prevent cyber-attacks or breaches before they happen.
- Cyber-resilience refers to an organization's ability to ensure and protect business continuity during the response and recovery stages of a cyber-attack or incident that disrupts business operations. Cyber-resilience implies and expects that breaches will happen, and it aims to prepare the organization for the least downtime and a quick, seamless recovery.

Figure 1. Cyber-Resilience vs. Cybersecurity

Emerging from the ashes of a cyber crisis with your reputation and assets intact is never a stroke of luck. Still, it directly results from a serious commitment to harness the synergizing power of cyber resiliency and cybersecurity. Investing in security talent and tools will complement cyber resiliency efforts and reinforce your cybersecurity initiatives. Effectively communicating the implementation of a proposed cyber-resiliency framework or strategy to your stakeholders can lead to buy-in contributing to the fullest return on that investment.

A good starting point for applying a framework can be observed in the main pillars set forth by the National Institute of Standards and Technology (NIST) Special Publication 800-160 for guidance on resilient cyber systems[i]. The pillars of the framework include Cyber Resiliency:

- Goals
- Objectives
- Techniques
- Implementation Approach
- Design Principles
- Solutions
- Mitigation

The relationship between each of these constructs and how they may be applied is also described in the framework. These constructs can be applied at levels surpassing the information or security system (e.g., mission or business functions, organizational or sector levels). They are useful for:

- Addressing and documenting high-level stakeholder priorities (i.e., Goal setting).
- Developing and interpreting metrics useful for vulnerability and cyber resiliency posture assessments (i.e., Objectives).
- Combining engineering and operational procedures, processes, and practices to meet stakeholders' needs and provide an adequate level of cyber resiliency to reduce risks to mission or business capabilities in the presence of advanced persistent threats (APTs) (i.e., Solutions).
- Integrating controls and solutions into information or security systems as they are used. This will reduce the risk of a cyber-attack or incident (i.e., Mitigation).

Gone are the days when an organization could cling to the false hope that deploying more security controls and tools provides adequate protection. While many vulnerabilities are widely known, commonly exploited, and routinely remediated with patching and vulnerability management programs, there are also the dreaded zero-day attacks and the intensifying prevalence of ransomware and extortion to consider.

Thriving in today's environment can require a doomsday survivalist mentality that enables you to envision and prepare for an ever-expanding threat landscape that is broad and complex. Cyber resiliency can lessen the sting and uncertainty of a surprise attack by taking much of the guesswork and human error out of your incident response (IR) and recovery.

LEFT AND RIGHT OF BOOM

The military uses the term "left of boom" to refer to defensive strategies which proactively prevent explosions and protect their assets and personnel from such a catastrophe. On the other hand, the term "right of boom" pertains to the events and strategic responses that occur in an explosion's aftermath. Regarding cybersecurity and cyber resiliency, you can see how the booming industries of ransomware and organized cybercrime also require tactics for firmly positioning your organization to the left and right of the "boom."

Preparing for the big bang can be daunting. Still, with the proper preparation and response playbook, you can reduce the likelihood of an attack and mitigate the impact of a successful one. The NIST Cybersecurity Framework (CSF)[ii] outlines the priorities you and your security talent should enact.

The NIST CSF outlines the process as follows:

Step 1 – Identify: Prioritize which processes and assets require protection (i.e., risk assessments, penetration testing, and management of policies, and assets).

Step 2 – Protect: Implement safeguards (e.g., awareness training, IR testing and tabletop exercises, access control, maintenance, and protective technologies) which ensure the protection of assets.

Step 3 – Detect: Implement mechanisms that monitor, identify, and alert your team of cybersecurity events and anomalies.

Step 4 – Respond: Implement IR plans for containing the impact of cybersecurity incidents. Identify areas of improvement.

Step 5 – Recover: Restore services and capabilities according to your IR plan and document the lessons learned for future improvements.

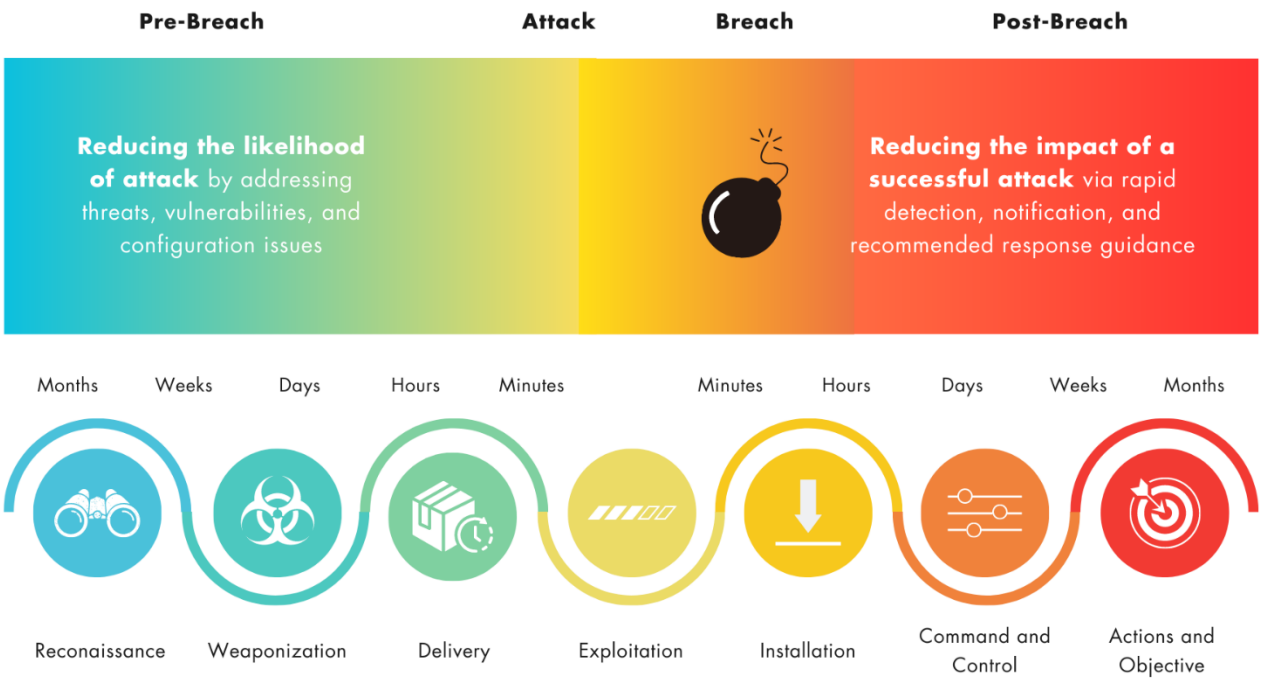

Figure 2. Left and Right of Boom

THE MODERN CIO

The CIOs of the future see the bigger picture. They are adaptable and lead with transparency, empathy, and a strategic vision. Ideally, the CIO will see cyber resiliency in a way that maintains a holistic understanding of the business, its customers, and its assets. With the heightened threat of organized cybercrime, the growing complexity and scale of digital transformation, and rising costs, your seat at the table places you at the helm of pivotal decision-making for technology budgets, strategic sales enablement tools, operational growth, and innovation.

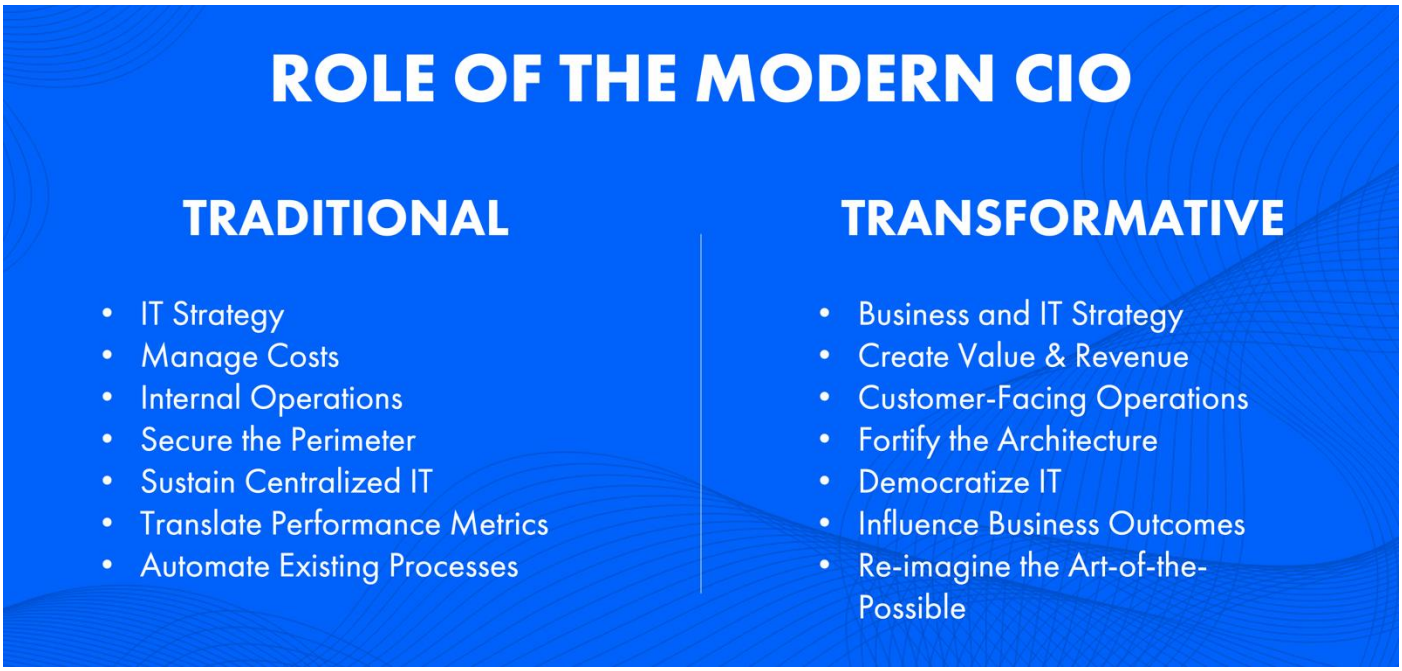

Figure 3. Role of the Modern CIO

The organization looks up to its leadership during the fallout of a cyber breach, so the CIO uniquely understands and accepts the weight of these decisions. As the CIO's responsibilities evolve and increase, their compensation has also risen, spiking 21% to $287,500 in 2022 compared to 2021, according to the Mondo firm[iii]. Technology will continue to see budget requirements climb because cybersecurity tooling and cyber resilience strategies are not one-and-done efforts. Projections reported by Gartner, Inc. forecast worldwide IT spending to rise by 2.4% in 2023, bringing total spending to $4.5 trillion[iv]. The growing breadth and depth of malicious actors and their capabilities will continue instigating these surges.

The ability to transfer or share risk with a managed security service provider (MSSP) or a cybersecurity insurance policy can be considered in those costs. Still, the availability and affordability of cybersecurity insurance vary by industry and business size. SMBs tend to have a harder time acquiring or justifying the necessary insurance due to dramatically rising premiums and stricter policy terms and conditions as underwriters are looking to cut their losses from skyrocketing claims.

There's no better time to advocate a cyber-resilient architecture. Confidently leading stakeholders into a new frontier of resiliency-focused outcomes for your organization starts with communicating the challenges, solutions, and long-term value of customized solutions for Business Continuity, Vulnerability and Risk Management, Cybersecurity, and other initiatives across your organization.

THE CHALLENGES

Business Leaders face many challenges...

Figure 4. Business Leaders' Challenges according to IDC[vi]

Cybersecurity-Specific Challenges

"By 2023, most C-suite leaders will implement business-critical KPIs tied to data availability, recovery, and stewardship as rising levels of cyberattacks expose the scale of data at risk."

Some of the most prominent roadblocks to integrating cyber-resilience in your organization's mission include:

- **Cybercrime**: In a time when it's commonly accepted that no one is 100% secure, the modern state of cybersecurity can make you long for the good old days when a fancy firewall and an antivirus vendor provided a sense of security. With digital transformations on the rise, the late 2000s observed a shift from thefts targeting physical records to a substantial rise in Personally Identifiable Information (PII) hacking[v].

  Cybercrime can result in devastating financial damage and even loss of competitive advantage. Whether the perpetrators are career criminals using ransomware to extort massive amounts of money, thieves stealing consumer or confidential data for personal gain, or politically motivated hacktivists carrying out DDoS attacks, the sky is the limit when considering the financial fallout. Compounded by the potential loss of proprietary data and consumer trust, the damage can be irreparable and far-reaching.

- **Complexity and Cost**: In the age of digital transformation (DX) the cyber footprint of SMBs has become increasingly complex and costly. Supply chain partnerships, migrations to the cloud, IT solutions, vendor training/support, and the race to facilitate secure remote work and resources in response to the COVID-19 pandemic all continue to increase in necessity while driving up costs. Weaving legacy systems into this ecosystem creates an even riskier expansion of the threat surface and potential costs. Oh, what a tangled web we weave.

- **Human Error**: Thanks to the increasing complexities described above, adding inadequate awareness training and the possibility of employee burnout to the equation increases the risk of human error. Particularly during the configuration or operation of IT solutions and networks. This vulnerability exposes yet another attack surface for bad actors to exploit. What's the worst that can happen? Unavailability of critical systems/services or the loss of valuable data.

- **Inadequate Planning**: You know how the saying goes, "Failure to plan is a plan to fail." Incident response planning is essential to recovery and business continuity in a cyberattack. Not having an established IR plan or relying on an untested or outdated plan can result in slower response times and may even increase or prolong the effects of an incident. Dropping the ball on planning is a play that directly opposes cyber resilience.

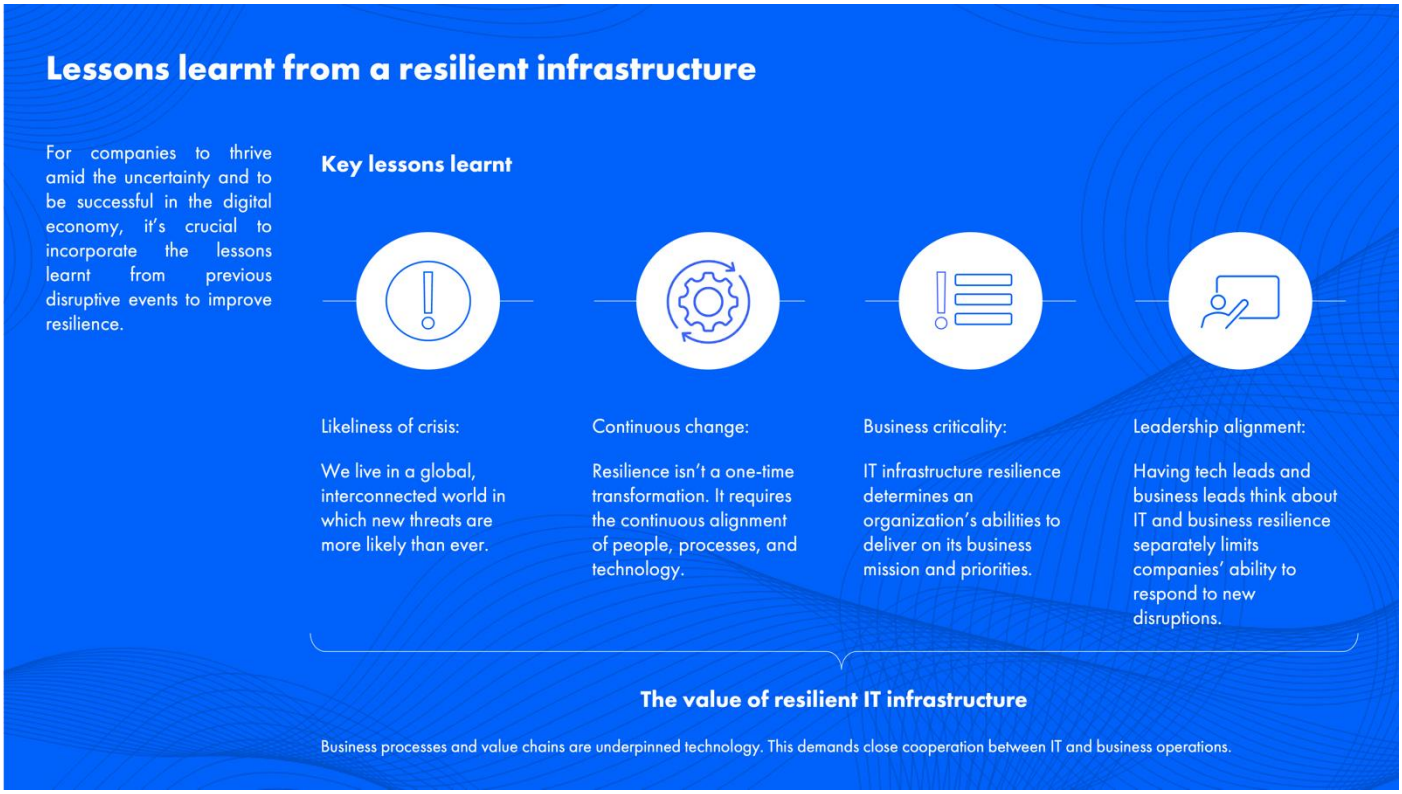

Figure 5. Lessons learnt from a resilient infrastructure[vi]

THE SOLUTIONS

Preparing for the "right side of boom" is within reach. Your teams may already be using cyber-resilient solutions.

- Mechanisms like automation, orchestration, and centralized data analysis for patching, software updates, onboarding or offboarding employees, and reporting may already be familiar tools used in your security operations. Applied strategically to disaster recovery and incident response, these time-saving solutions can streamline and optimize cyber resiliency efforts by providing more visibility and control.
- Changing mindsets to redirect focus on reducing complexity and normalizing simplicity will create a new and improved blueprint for a cyber-resilient organization. CIOs, stakeholders, and managing leaders who are intentional and transparent about their long and short-term goals toward cyber resiliency should begin to reap the benefits of a simpler ecosystem. Ideally, using more recent cybersecurity solutions or an MSSP, paired with current best practices in policy and procedure, will provide added interoperability and integrations on your networks and systems.
- Collaborate with all levels of leadership to develop, document, and test an Incident Response Plan and Business Continuity Plan. These plans should prioritize the most prevalent risks identified by current risk assessments and vulnerability reports. The plans will include all points of contact (POC) for incident response, law enforcement contacts, guidelines specifying the types of incidents requiring reporting, and the POCs to report to.

Established deadlines for response times, written procedures for emergency disaster recovery, and tested methods for restoring backups, which have also been tested for viability. At least tabletop exercises with all related teams and relevant personnel should be conducted annually. Lastly, share and document the lessons learned after a cyber incident to reinforce awareness and continued improvements.

Your organization's ability to withstand threat actors and quickly restore business operations after a breach translates into the transformational awareness and readiness that cyber resiliency cultivates. The proper framework will enforce better practices companywide while adopting preventative strategies and preparatory measures which can sustain and justify the necessary budget for resources, talent, and partnerships in Information Security, Cybersecurity, Business Continuity, Vulnerability Management, and other instrumental Information Security disciplines across your organization.

Figure 6. Cyber Resiliency Solutions

Click here for more information about seeing these solutions in action when you trust DataGuard to lead your organization's cyber resiliency endeavors with the exceptional cyber defense capabilities now offered to the private sector. With our unique data assets, world-class threat intelligence experts, and managed security services, we are proud to provide organizations of all sizes with the same level of cybersecurity that was previously available only to the largest and most well-defended businesses and government agencies. We accomplish this by focusing on preventative and proactive security coupled with the latest technology in AI, Vulnerability Assessments, Cyber Awareness Training, Policy and Procedure Development, and 24/7 live SOC monitoring[vii].

Author:

Christopher Zvirbulis
Chief Commercial Officer/Partner at Data-Guard365, Inc.

27-year career in Technology, Non-Profit Board Member, Father and Husband

REFERENCES AND CITATIONS

[i]National Institute of Standards and Technology, 'NIST SP 800-160 vol. 2, rev. 1, Developing Cyber Resilient Systems', NIST, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (accessed March 8, 2023).
[ii]National Institute of Standards and Technology, 'NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1', NIST, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed March 9, 2023).
[iii]Wall Street Journal (WSJ), 'CIO Pay Jumps as Tech Moves Closer to Core of Business', WSJ, 2022, https://www.wsj.com/articles/cio-pay-jumps-as-tech-moves-closer-to-core-of-business-11645534801 (accessed March 10, 2023).
[iv]Gartner, Inc., 'Gartner Forecasts Worldwide IT Spending to Grow 2.4% in 2023', Gartner Press Release Newsroom, 2023, https://www.gartner.com/en/newsroom/press-releases/2023-01-18-gartner-forecasts-worldwide-it-spending-to-grow-2-percent-in-2023 (accessed March 10, 2023).
[v]Chase, Abigail, 'The Evolution of Cyber Risk and the Cyber Insurance Market', Senior Theses, 2021, https://scholarcommons.sc.edu/senior_theses/412/ (accessed March 10, 2023).
[vi]International Data Corporation, Building Resilience in a Digital-First World, https://www.idc.com/ (accessed March 28, 2023)
[vii]Data-Guard365, 'Digital Workspace Solutions', DG365, 2023, https://data-guard365.com/digital-workspace-solutions/ (accessed March 11, 2023).