

2023

MEASURING AND MANAGING CYBER RESILIENCE






REVEALRISK

MEASURING AND MANAGING CYBER RESILIENCE

Resiliency in cybersecurity is not a new concept. It has long been postulated as a goal or used to convey that a business needs to be ready for the unpredictable that can and will arise in a volatile cyber-risk climate. However, we have seen that there is a disconnect between current practices for evaluating & leading cyber programs, and understanding, measuring, & building true cyber resiliency.

Related to the concept of resilience, let's look at terms to get some grounding in concepts. According to dictionary.com, resilience means:



resilience [ri-zil-yuhns, -zil-ee-uhns] [SHOW IPA](#)  

[See synonyms for resilience on Thesaurus.com](#) Middle School Level

noun

- 1 the power or ability of a material to return to its original form, position, etc., after being bent, compressed, or stretched; [elasticity](#).
- 2 the ability of a person to adjust to or recover readily from illness, adversity, major life changes, etc.; [buoyancy](#).
- 3 the ability of a system or organization to respond to or recover readily from a crisis, disruptive process, etc.:
Cities can build resilience to climate change by investing in infrastructure.

All three definitions are relevant to cybersecurity because holistic cybersecurity requires a symbiotic connection between people, processes, and technology.

Cyber Resilience (according to NIST) is “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

A BOXING ANALOGY WOULD BE THE ABILITY TO TAKE THE PUNCH AND STAY STANDING, KEEP MOVING,



OR GET UP FROM BEING KNOCKED DOWN.



Many modern organizations use a maturity framework to evaluate the current state of their program, set goals of areas to enhance, obtain the necessary funding, and measure performance over time. Popular choices include the NIST CSF (Cybersecurity Framework) or ISO27001 which both provide industry-accepted criteria and enable benchmarks to peers and other organizations.

These frameworks are helpful in identifying what key elements are in place and the relative maturity of each. Companies will measure their maturity using a scoring rubric such as CMMI (Carnegie Mellon Maturity Index 1-5 rating or similar methods) to get an aggregate score representative of process or capability definition, process documentation, measurability, and ability to continuously improve).

While very helpful for setting direction and monitoring progress, these models have gaps and assessors sometimes *neglect to measure*.

- The scale or coverage of technical tool implementations and critical process controls across the entire company and critical assets.

- Business ownership, business buy-in, and cross-functional integration for security-relevant processes and services.
- Live testing, rehearsals, and other measures of operational effectiveness for critical processes and controls.

This doesn't mean you should scrap your maturity framework! Just as no single cybersecurity tool will ever be a silver bullet that solves every problem (no matter how many marketing and sales folks may wish it), a maturity framework won't answer every question an executive may ask or a cybersecurity leader may need to proactively consider.

Examples:

- How effective would we be in responding to and recovering from a major cyber-attack?
- Do our most effective controls, processes, and technology cover all of what is most critical to our business and operations?
- How do we (or can we) continue business operations during a major cyberattack?
- Do we have any disconnects between business areas, core functions, or divisions that could cause breakdowns or otherwise impair our response and recovery efforts during a cyber-attack?

An effective Cyber Resilience program should build upon the basics of your broader program and this includes your maturity model. As we have seen across a variety of clients and industry sectors while conducting cybersecurity incident response “war games” or tabletops, simulations can prompt leaders to consider scenarios and questions that maturity frameworks and cybersecurity tool/process implementations do not address. Capability gaps, holes in tool coverage, communications breakdowns between process owners, uniqueness at regional sites or acquired entities/divisions, and simple human behavior during a crisis are not things that a maturity score will necessarily reveal.

In a recent discussion with several Fortune 500 CISOs, we recognized a growing need for a way to deepen the ability to answer core questions around cyber resilience and being best positioned to recover effectively after a cyber attack. Working with a trusted panel of CISOs, industry experts and our own experienced leadership team at


Reveal Risk, we have developed a playbook and program implementation approach that helps organizations identify these gaps, articulate their cyber resiliency, readiness for incidents, and track their ability to recover or return to normal business operations.

Since cybersecurity resilience is not a new topic, we wanted to make sure we leveraged what's already come before. Aside from not wanting to reinvent the wheel, we want to ensure that the model is relevant for organizations that have progressed their resiliency journey as well as those who are just beginning it.

Cybersecurity Program/Maturity Frameworks

- **NIST CSF** (Cyber Security Framework)
- **ISO/IEC 27001** and **ISO 27002**
- **HITRUST CSF** (healthcare focus)
- **Cybersecurity Maturity Model Certification - CMMC** (US federal subcontractor focused)

The Good

- 
- These are solid foundations for measuring cyber program coverage, giving organizations a 1-4 or 1-5 scaled maturity score, and helping to build a program roadmap to address any fundamental capability gaps.
 - A cyber resilience program can (and should) be built in alignment with your maturity framework so that you are not creating duplication or rework. A Program Maturity framework and correlated program design/roadmap are holistic across many information security risks.
 - We see the NIST CSF most commonly used in the US to measure program maturity and guide prioritization.
 - NIST CSF is free to use and has broad support in the cybersecurity industry.
 - ISO is more popular for international companies that require or desire a formal certification against the ISO framework.
 - HITRUST is emerging as a common framework for healthcare providers regulated by HIPAA, but it can be expensive and niched to healthcare.
 - We see many organizations turning to a SOC 2 Type 2 audits of their controls (often aligned to NIST controls) to provide independent verification of their controls similar to ISO or HITRUST certifications.

The Gaps



- These maturity frameworks don't do a good job of evaluating the scale and effectiveness of your program elements.
- Maturity frameworks tend to recognize programs that invest in capabilities and robust process documentation, but they are inconsistent in assessing coverage and effectiveness.
- Additionally, they don't provide consistent mechanisms for identifying wasteful or unnecessary components and investments.

Cybersecurity Resilience Focused Frameworks and Assessments

- NIST Special Publication 800-160 CISA / Carnegie Mellon Cyber Resilience Review (CRR)
 - The CRR is supported by the CERT RMM (Resilience Management Model)
- Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (SSECMAETSS)

The Good



- NIST and CISA jointly publishing guidance for cyber resilience is a strong reinforcement of the concept and points to potential future investments.
- The CRR is aligned to the NIST CSF framework and includes a comprehensive mapping between both. This helps it to be more additive than competing or contradictory.
- The RMM is the instructional detail behind the components of the CRR. It weighs in at ***a whopping 860 pages***.
- The SSECMAETSS guidance is a solid approach for building secure design principles into the early stages of systems development. This principled focus is an often discussed, rarely implemented ideal since influencing busy IT teams can be difficult and many organizations do not have the right incentives to accomplish what is needed.

The Gaps



- The NIST/CISA publication was released quietly during the early days of the COVID-19 pandemic and seems to have suffered as a result. There is currently very limited support from vendors and we were not able to find much evidence of adoption outside of the federal sector (this could be because of the size and complexity of the materials)
- NIST creates a labyrinth of references between special publications and additional resources that organizations must traverse to understand the full implications of following the guidance
- Both publications lack the necessary elements for measuring scale, coverage, and prioritization of what organizations value most. Overall, they should be considered more like NIST CSF sub-set assessment tools to expound on cyber resilience-focused control areas.

Reveal Risk Cyber Resilience Simplified Methodology and Playbook

Taking an appreciation for what has already been done, we at Reveal Risk set out to define a simplified approach to understanding, communicating, and actioning foundational cyber resilience elements. We want to create a way to clearly articulate cyber resilience in a way that avoids miscommunication, drives good investments, and aligns executive support with critical needs.

Our simplified approach/playbook takes elements from the existing frameworks and breaks them down into straightforward concepts that are more understandable and consumable by non-technical leaders.

01

IDENTIFY AND PROTECT

KNOW WHAT YOU ARE DEFENDING

- Risk Management and Controls
- Vulnerability Management and Patching
- Third-Party / Supply Chain Risk Management
- Workforce Awareness and Human/Process Controls
- Protect Critical and Legacy Assets

Our approach consists of the following high-level elements that summarize critical concepts from thousands of pages of frameworks, supporting references, and supplemental publications:

- **3** Key Strategic Focal Areas (aligned to NIST CSF)
- **10** Cyber Program Elements
- **20** Actions/Measures

03 **RESPOND AND RECOVER**
DEFINE AND PRACTICE RESPONSE EFFORTS

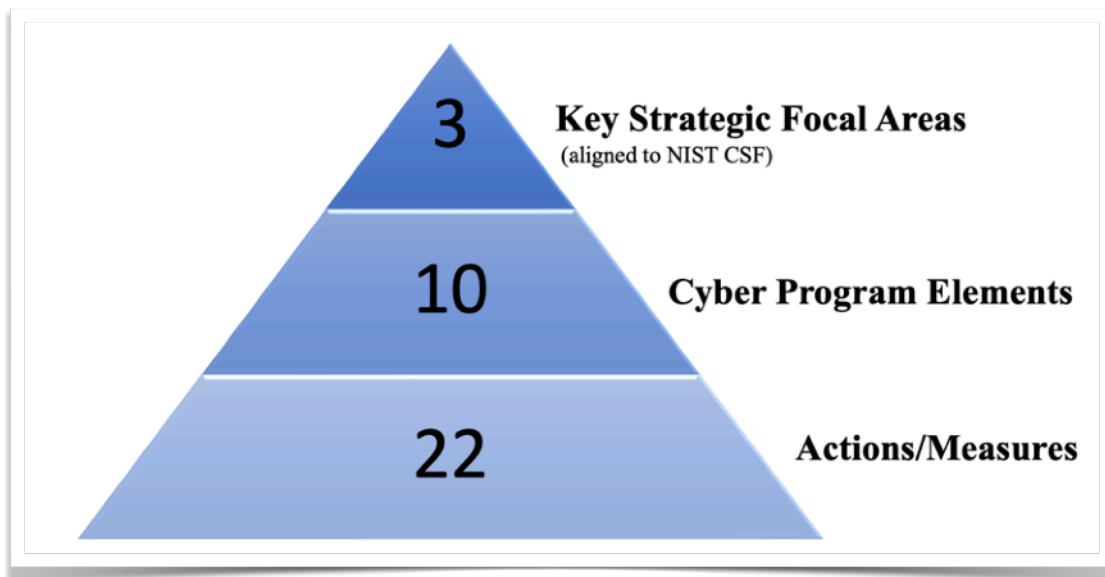
- Response Plans and Linkages
- Practice/Rehearse Response Plans
- Backup and Restore Processes

Improvement

- SOC (Security Operation Center) / SFC (Cyber Fusion Center) routine practice

Each of these layers is highly actionable and measurable across the prioritized scale that you need to implement them across. The goal is to define how resilient you might be to a major cyber event, and specifically where you need to get better.

Reveal Risk Cyber Resilience Playbook



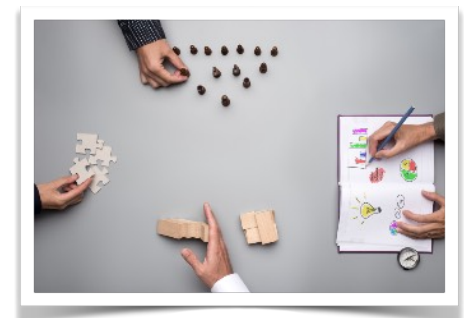
1 *Know what we are defending – Identify and Protect*

A. Risk Management and Controls

- **Know your top business risks and crown jewels** so you can map them in the context of cyber incidents or insider threats. This involves information classification and handling guides, but extends beyond this because many business processes are critical from an availability standpoint (even if they don't contain sensitive company or personal information).
- **Define controls for what you care most about** and how you plan to implement them across critical IT assets, third parties, and business processes.

B. Vulnerability Management and Patching

- **Identify assets beyond the crown jewels to inform VRM and patching processes.** Identification of crown jewels is priority one, but without a clear understanding of the other assets in an organization's environment, identifying vulnerabilities and patching assets becomes a challenge. Vulnerabilities in non-critical or crown jewel supporting assets can ultimately impact critical processes.
- **Build great process and governance for your vulnerability scanning to set the right priorities and create accountability to remediate or patch –** with risk-based prioritization of the most impactful gaps from a business-risk and technical severity standpoint, security creates more engagement without it seeming like everything is broken and everything is important. VRM programs can easily become “white noise” creating frustration for both sides. Focusing on what matters most first doesn't mean stopping at the top of the pyramid. It does, however, give a more rational starting place and allows expanding later instead of forcing a “shotgun” approach.



C. Third-Party / Supply Chain Risk Management

- **Identify and manage risks in the most critical third parties** to the organization including those the data, technology, or source code supply chain. Build a capability to identify, remediate, monitor and govern risks related to third parties (with efforts aligned to the business risk of the third party). Similar to internal vulnerability management, start with what is most critical and expand from there.

D. Workforce Awareness and Human/Process Controls

- **Define secure behaviors, expectations, and controls for all employees.** This goes further than helping the workforce be “aware”, and dives into the actions that they need to individually do to protect the information they handle and the critical operations they support. Your workforce cannot help you protect the company if you cannot clearly articulate what you need them to do and *why*.
- **Map and tighten critical business processes, focusing on human behaviors and actions.** This is an often-missed activity because it involves digging into critical business processes outside of IT and security. We believe that this is one of the best developmental areas for cyber professionals. It is also an amazing way to build networks of champions within business areas that can be an extension of your program.
- **Equip the workforce to quickly report concerns as they encounter them.** The biggest challenges on this front are programs not being clear about how to report concerns, and not answering the common fear that reporters will get in trouble if they report something that they could be blamed for.



E. Protect and Confine Critical and Legacy Assets

- **Design and implement network controls to protect critical and legacy assets.** Segmenting critical assets is one of the most important things organizations can do to protect them. End-of-life assets along with built-for-purpose assets, such as operational technology and IoT devices also need to be considered when developing a segmentation. Like other areas in the cyber domain, prioritization is the key success factor. Business risk identification can help inform segments.



2 *Monitor and detect cyber events - Detect*

A. Cyber Tool and Tech Architecture

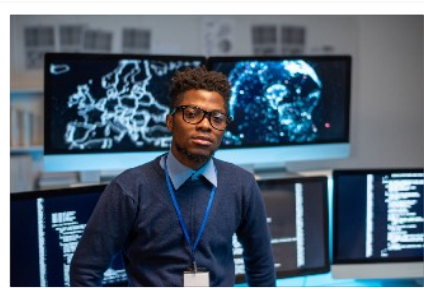
- **Map cyber tools and technical capabilities against a cyber architecture framework:** Identify gaps, redundancy, and scale of coverage. Add and *subtract* from your tool stack to rationalize and improve focus. Three tools with great adoption and scale are almost always more effective than ten tools with mediocre adoption and scale. There are no points for excess purchases. What you do to optimize your operating budget and cyber tooling will make all the difference to your cyber resilience (and overall mental load).

B. Cyber Tool and Tech Continuous Improvement

- **Measure cyber tool effectiveness measurement:** You cannot improve what you do not measure. Solid measures of tool effectiveness, such as deployment, and false-positive rates, help ensure that cyber programs continue to improve with their existing toolsets and reduce the need to major pivots or upgrades. Lacking good metrics, many programs tend to underfund “last year’s” efforts. The result becomes a cyber program that is a never-ending treadmill of chasing *what is next*, and neglecting *what is now*. Most cyber-attacks compromise “the basics”, yet many leaders and programs spend the majority of their time on what is sexy. So sexy, it hurts.

C. Security Operation Center (SOC) / Cyber Fusion Center (CFC) routine practice

- **Practice (internal to Info Sec) routinely** – through real events or mock drills.



These should be regular, informal, and often (as opposed to executive or cross-functional table-tops and war games, which take more planning and investment). The idea here is to get teams to see the value of communication, practice, and wiki-style run books. They are all about promoting collaboration, teamwork, and embedding muscle memory so the team can be great under the pressure of real incidents.

3 *Define and practice response efforts - Respond and Recover*

A. Response Plans and Linkages

Each of these plans is important and may be combined/integrated where it makes sense. The most important aspect is making sure actions, coordination, and roles & responsibilities are clear. If all of these plans are not in place, prioritize the Cyber Incident Response Plan and Disaster Recovery Plans.

- **Cyber Incident Response Plan** – A good cyber incident response plan is a cross-functional, executive-level guide that identifies clear roles and responsibilities. The plan includes playbook-level cues for key questions and topics that might get missed during a high-stress incident.
- **IT Incident Response Plan** – An IT incident response plan must be broad enough to cover many types of IT incidents and outages (including cyber events). It is important to design it in a way that compliments other plans such as the cyber incident response plan and doesn't compete with them. A common organizational pitfall is having this plan created independently of other teams.
- **Corporate Crisis Management Plan** – This may not be necessary for all companies, but where it is, it's usually owned by physical security, legal, or corporate communications. The plan deals with a wide variety of company crises and how to respond to them. It is important to understand and define integrations to the cyber incident response plan. Typically the crisis management plan is activated for the most serious events only.
- **IT Disaster Recovery Plans** – The IT disaster recovery plan helps IT plan for how they would recover from a broad disaster, ideally including a widespread cyber-attack. It weaves together processes, tools, and capabilities (like DRaaS – Disaster Recovery as a Service), backup and restore capabilities, or other automated technologies to recover data,



systems, and networks. Within the cyber incident response plans and related rehearsals, it is important to understand coverage and gaps that might impair resilience and recovery. Disaster recovery plans should be tested regularly to identify “glitches” such as silently failing backups before a real disaster.

- **Business Continuity Plans** – Each critical business process should have a continuity plan. The plan needs to be owned and managed by accountable business leaders. BCP programs that are owned within IT and lack business engagement are usually not worth the paper they are written on. One large company that suffered a very public cyber event (NotPetya), causing many business operations to shut down for extended periods of time. They had a well-funded, IT-owned BCP program that was completely scrapped and reconstructed by senior executives during the crisis because it did not have the right involvement, accuracy, and ultimately it couldn’t be executed when the crisis hit.

B. Practice/Rehearse Response Plans

- **Tabletops, Rehearsals, and Simulations:** Practice may not make perfect, but it is the only way to improve. Practice in the form of a tabletop, rehearsal, or simulation will help you add elements but oftentimes simplify processes and execution. If a plan is not used and referenced during practices or real events, it is not adding value. It is valuable to start simple and add complexity over many iterations through practicing.



C. Backup and Restore Processes

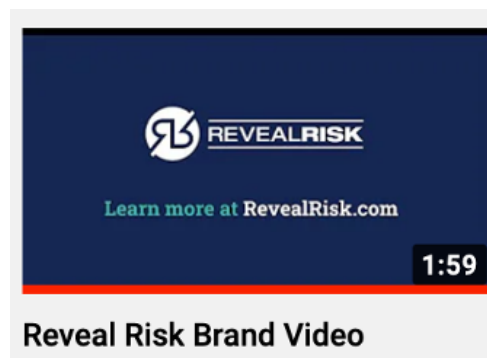
- **Define Backup & Restore technology** – Your overall ability to backup and restore is limited by the technology options you have (DRaaS, hot-sites, cloud backups, etc.). Your technology should deliver appropriate capabilities based on business needs as identified in a Business Impact Assessment (BIA) as part of Business Continuity Planning.
- **Define processes** - Make choices clear, and adoption paths and processes as simple as possible for all stakeholders. Early IT project investment costs and timeline can be barriers to getting the right scale of B&R technology implemented. Focus on what is most important first.

- **Scale and dashboard/report coverage** -Having easily accessible and accurate information about what is backed up, how, and how often across IT assets is a key dependency of effective incident management. This is especially true when a cyber attack impacts availability and data, such as ransomware.
- **Test ability to restore** – If you haven't tested it, can it be trusted to work during a high-stakes incident? This is a rhetorical question, but so many companies have discovered the answer to this one after it was too late. Pick a sample of assets and data repositories, by type and technology, and test your tech and processes regularly.



Do you want to explore how Reveal Risk could help you define a plan and implement a cyber resilience-focused program within your organization? At Reveal Risk, we evaluate, design, and deliver strong cybersecurity programs, processes, and results in cybersecurity. We can bring Cyber Resilience to life in your organization in a focused manner that works within your organizational structure, culture, and budget reality.

[Learn More About Our Story!](#)



CONTACT US!

REVEALRISK.COM
650 E CARMEL DR. SUITE #340
CARMEL, IN 26240
317-759-4453
INFO@REVEALRISK.COM

