Cyberresilience in an Evolving Threat Landscape

It is important to know if one's organization is robust enough to survive in the event of a security event, let alone expand and improve. Many reputable cybersecurity organizations are publishing guidance on how to respond in the event of a theft or data breach. If sensitive enterprise data or accounts have been compromised because of theft or loss of a laptop, smartphone or other device, or because of a breach of network security or an account, actions to take include:[1]

- Reporting the loss or breach to IT or security personnel immediately, and to the bank when appropriate
- Changing all passwords used to log on to the affected device
- Contacting the service provider for help in wiping the data from affected smartphones and other mobile devices

From an engineering point of view, it is also helpful to know how to maintain the ability to "anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyberresources."[2] An organization can identify and plan use cases to test its cyberresilience as it matures its baseline level or approach, and it can spend an inordinate amount of funds to protect its infrastructure and other related assets. However, there is no guarantee that an organization can withstand and adapt to adverse events.

The digital world has revolutionized how people live, work and play. However, it's a digital world that is constantly open to attack, and because there are so many potential attackers, it is necessary to ensure that the right security is in place to prevent systems and networks from being compromised. Unfortunately, there is no single method that can successfully protect against every single type of attack. This is where a defense in depth (DiD) architecture comes into play.[3]

DiD is "an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. DiD is commonly referred to as the castle approach because it mirrors the layered defenses of a medieval castle. Before a castle can be penetrated, attackers face moats, ramparts, draw bridges, towers, battlements and other defenses.[4]

Larry Marks, CISA, CRISC, CGEIT, CFE, CISSP, CSTE, ITIL, PMP
Has focused his career on leading through collaboration to ensure that best practices are implemented to assist compliance and process improvement. He has focused on audit, security, risk, compliance, privacy and program/project management across financial services, healthcare and telecommunications. Marks has extensive experience in designing, managing, auditing and implementing IT processes, policies, controls and technology. He has managed teams, priorities and expectations across business and IT leadership while delivering fit-for-purpose services. He is a peer reviewer for the *ISACA® Journal* and the Association of Certified Fraud Examiners (ACFE) *Fraud Magazine*. Marks is also associate editor for *Information Security Journal: A Global Perspective*, published by (ISC)², and contributes book reviews to *InfoSecurity Professional*. Marks was recently selected to be a member of the Rutgers University Cyber Advisory Council (New Brunswick, New Jersey, USA). He currently holds a leadership position in the ACFE New Jersey (USA) chapter. He has contributed to ISACA® white papers and has authored/coauthored ISACA audit programs. Marks served on the Certified in Risk and Information Systems Control® (CRISC®) exam-writing team and is part of the Project Management Institute's ISO Committee. He is also a blogger and contributor to the leadership section of ProjectManagement.com. His work has been published in the *(ISC)² Security Journal*, the *PMI Journal* and the *ISACA Journal*.

Other than DiD, the current approach that professionals are discussing is to expect that a cyberattacker has been in the organization's environment and remains there, waiting for the security professional to uncover the attacker through various means. How can the organization anticipate and recover from the stresses of a relentless attacker such as a nation-state?

The US National Institute of Standards and Technology (NIST) issued guidance that recommends organizations "bake in" cyberresilience to their policies, processes, procedures and applications. Organizations should ensure that cyberresilience is a priority during their systems development life cycle, from architectural decisions to stakeholder requirements. The NIST guidance can be used to identify a practical approach for its application. For example, should cyberresilience be implemented for all systems or only critical systems?

How Cyberresilience Differs From Other Types of Contingency Planning

Cyberresilience refers to the operational response and recovery planning efforts stemming from a cyberattack. Although the concept of cybersecurity has matured into an accepted profession and a component of a good risk technology program, cyberresilience is an evolution in maturity. In a way, it follows the evolution of business continuity as a separate and distinct idea from IT disaster recovery.

Incident management is the process of managing IT service disruptions and restoring services within agreed service level agreements (SLAs). "The scope of incident management starts with an end user reporting an issue and ends with a service desk team member resolving that issue."[5] Enterprises developing or testing their incident management generally develop a limited set of use cases to ensure a consistent and effective approach in the event of a security breach, determine how their infrastructure can respond and identify how to improve this process. The enterprise then convenes a lessons learned session to ensure that it was able to recover from the incident in a timely and effective manner.

> "ALTHOUGH THE CONCEPT OF CYBERSECURITY HAS MATURED INTO AN ACCEPTED PROFESSION AND A COMPONENT OF A GOOD RISK TECHNOLOGY PROGRAM, CYBERRESILIENCE IS AN EVOLUTION IN MATURITY."

Alternatively, many organizations have issued guidance on continuity planning.[6] IT continuity planning is the process of ensuring continuous operations of business applications and supporting IT systems (e.g., desktops, printers, network devices). IT continuity planning is a subset of enterprise business continuity planning (BCP). A business continuity plan is an enterprisewide group of processes and instructions used to ensure the continuation of business processes in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents (e.g., localized disruptions of business components) and major disruptions (e.g., fire, natural disasters, extended power failures, equipment or telecommunications failure). The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise.

The IT continuity plan addresses IT exposures and solutions based on the priorities and framework of the business continuity plan. The role of the IT audit/assurance function is to provide assurance that the risk has been addressed by the business/IT owners. As a best practice, the business continuity plan should be evaluated for any guidance addressing its framework, priorities, responsibilities and objectives.

The IT continuity plan must be aligned with the business continuity plan to ensure that:

- Risk is appropriately identified and evaluated by focusing on the impact on business processes for known and potential risk
- The costs of implementing and managing

continuity assurance are less than the expected losses and within management's risk tolerance

- The business priorities are addressed (i.e., critical applications, interim processes, restoration activities, mandated deadlines)
- Manual interfaces to automated processes are identified, personnel are trained and practice drills are conducted
- Expectations are managed with realistic goals

Why is the difference between cyberresilience, BCP, IT continuity planning and incident response planning important?

- There is currently an emergence of cyberresilience, which is seen as a discipline that can be impacted and influenced by related programs. These related programs include cybersecurity, IT disaster recovery, BCP, crisis/incident management, and third- and fourth-party risk management.
- Cyberresilience goes beyond the typical prevent, detect and respond models found in cybersecurity and requires an operational resilience program to ensure that critical business processes can recover from cyberattacks with minimal disruptions and within prescribed recovery time objectives.
- Cyberresilience requires enterprises to consider threats and risk that may impact their enterprise risk framework and the frameworks of their third-party suppliers and vendors.

Why Is NIST Guidance Important?

NIST expanded its guidance to ensure that organizations' goals, strategies and systems incorporate cyberresilience analysis and approach. NIST suggests that the objectives of cyberresilience are prevent or avoid, prepare, continue, and constrain (**figure 1**).[7]
These objectives cover several areas, including:

- **Analytic monitoring**—Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.
- **Contextual awareness**—Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action.
- **Coordinated protection**—Ensure that protection mechanisms operate in a coordinated and effective manner.
- **Deception**—Mislead, confuse, hide critical assets from or expose covertly tainted assets to the adversary.
- **Diversity**—Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.
- **Dynamic positioning**—Distribute and dynamically relocate functionality or system resources.
- **Nonpersistence**—Generate and retain resources as needed or for a limited time.
- **Privilege restriction**—Restrict privileges based on attributes of users and system elements as well as on environmental factors.
- **Realignment**—Align system resources with current organizational mission or business function needs to reduce risk.
- **Redundancy**—Provide multiple protected instances of critical resources.
- **Segmentation**—Define and separate system elements based on criticality and trustworthiness.

Figure 1—Cyberresiliency Objectives

Objective	Description
Prevent or avoid	Preclude the successful execution of an attack or the realization of adverse conditions.
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity.
Continue	Maximize the duration and viability of essential mission or business functions during adversity.
Constrain	Limit damage from adversity.

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Figure 2—Cyberresiliency Sub-Objectives

Objective	Representative Sub-Objectives	Representative Examples of Metrics
Prevent or Avoid Preclude the successful execution of an attack or the realization of adverse conditions.	• Apply basic protection measures and controls tailored to the risks of the system-of-interest. • Limit exposure to threat events. • Decrease the adversary's perceived benefits. • Modify configurations based on threat intelligence.	• Time to patch or to apply configuration changes. • Percentage of resources for which configuration changes are made randomly. Percentage of resources for which lifespan limits are applied. • Percentage of sensitive data assets that are encrypted. Adversary dwell time in a deception environment. • Percentage of resources to which more restrictive privileges are applied automatically in response to threat indicators.
Prepare Maintain a set of realistic courses of action that address predicted or anticipated adversity.	• Create and maintain cyber courses of action. • Maintain the resources needed to execute cyber courses of action. • Validate the realism of cyber courses of action using testing or exercises.	• Number of cyber courses of action (CCoAs) in the cyber playbook. Percentage of identified threat types, categories of threat actions, or TTPs (with reference to an identified threat model) addressed by at least one CCoA in the cyber playbook. • Percentage of cyber resources which are backed up. Time since last exercise of alternative communications paths. Percentage of administrative staff who have been trained in their CCoA responsibilities. • Time since last (random, scheduled) exercise or simulation of one or more CCoAs.
Continue Maximize the duration and viability of essential mission or business functions during adversity.	• Minimize degradation of service delivery. • Minimize interruptions in service delivery. • Ensure that ongoing functioning is correct.	• Time to perform mission or business function damage assessment. Length of time performance of specified mission or business function remained below acceptable levels. • Time from initial disruption to availability (at minimum level of acceptability) of essential functions. • Percentage of essential data assets for which data quality has been validated. Percentage of essential processing services for which correctness of functioning has been validated.

- **Substantiated integrity**—Ascertain whether critical system elements have been corrupted.
- **Unpredictability**—Make changes randomly.

The two cyberresilience techniques that only address adversarial threats are deception and unpredictability. Cyberresilience techniques are also interdependent. For example, the analytic monitoring technique supports contextual awareness. However, the unpredictability technique is different from the other techniques in that it is always applied in conjunction with some other technique, for example, working with the dynamic positioning technique.

Figure 2 illustrates samples of metrics or key performance indicators (KPIs) that can be used to measure the overall objectives of cyberreslience. In fact, each of the main cyberresiliency objectives can be decomposed into sub-objectives to facilitate measurement, management, tracking and prioritization.

The use of NIST 800-160 objectives requires an organization to be proactive in its cyberresiliency approach and process. The NIST approach expands and matures the strategies identified by (ISC)^2 as

> “THE ORGANIZATION MUST DEVELOP AN INVENTORY OF USE CASES FOR CYBERRESILIENCE THAT IS APPLIED TO BUSINESS PROCESSES”

Figure 2—Cyberresiliency Sub-Objectives *(cont.)*

Objective	Representative Sub-Objectives	Representative Examples of Metrics
Reconstitute Restore as much mission or business functionality as possible after adversity.	• Identify untrustworthy resources and damage. • Restore functionality. • Heighten protections during reconstitution. • Determine the trustworthiness of restored or reconstructed resources.	• Time to identify unavailable resources and represent damage in status visualization. • Time between initiation of recovery procedures and completion of documented milestones in the recovery, contingency or continuity of operations plan. Percentage of cyber resources for which access control is maintained throughout the recovery process. • Percentage of cyber resources for which additional auditing or monitoring is applied during and after the recovery process. Time to bring online a backup network intrusion detection system. Percentage of reconstituted cyber resources which are placed in a restricted enclave for a period after reconstitution. • Percentage of restored or reconstructed (mission-critical, security-critical, supporting) data assets for which data integrity/quality is checked.
Understand Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.	• Understand adversaries. • Understand dependencies on and among systems containing cyber resources. • Understand the status of resources with respect to threat events • Understand the effectiveness of security controls and controls supporting cyber resiliency.	• Time between receipt of threat intelligence and determination of its relevance. Adversary dwell time in deception environment. • Time since most recent refresh of mission dependency or functional dependency map. Time since last cyber table-top exercise, Red Team exercise, or execution of controlled automated disruption. • Percentage of system elements for which failure or indication of potential faults can be detected. Percentage of cyber resources monitored. • Number of attempted intrusions stopped at a network perimeter. Average length of time to recover from incidents.
Transform Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively.	• Redefine mission/business process threads for agility. • Redefine mission/business functions to mitigate risks.	• Percentage of mission or business process threads which have been analyzed with respect to common dependencies and potential single points of failure. Percentage of mission or business process threads for which alternative courses of action are documented. • Percentage of essential functions for which no dependencies on resources shared with non-essential functions can be identified. Percentage of problematic data feeds to which risk mitigations have been applied since last analysis.
Re-Architect Modify architectures to handle adversity and address environmental changes more effectively.	• Restructure systems or sub-systems to reduce risks. • Modify systems or sub-systems to reduce risks.	• Size of the (hardware, software, supply chain, user, privileged user) attack surface. Percentage of system components for which provenance can be determined. Percentage of system components which can be selectively isolated. • Percentage of cyber resources for which custom analytics have been developed. Percentage of mission-critical components for which one or more custom-built alternatives are implemented.

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

part of the Cybersecurity Workforce Study, which studied the cybersecurity workforce, gap estimates and insights into methods for building a resilient team now and in the future.[8]

The Impact of NIST 800-160 on an Enterprise

When considering the topic of cyberresilience in relation to NIST 800-160, the question to answer is what are the key components, objectives and means to implement the guidance. How does this layer onto the cyberstrategies of information security and the enterprise in general? NIST 800-160 provides an approach through the use of cyberresiliency constructs (**figure 3**). Specifically, enterprises can optionally select and implement the cyberresilience objectives, metrics and approaches on a phased approach as they meet the enterprise's needs and risk assessment.

NIST provides examples of cyberresilient approaches as illustrated in **figure 4**.[9]

Figure 3—Cyberresiliency Constructs

Construct			Definition, Purpose, and Application at the System Level
Goal			**Definition:** A high-level statement supporting (or focusing on) each aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyberresiliency. **Purpose:** Align the definition of cyberresiliency with definitions of other types of resilience. **Application:** Can be used to express high-level stakeholder concerns, goals or priorities.
Objective			**Definition:** A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security; the objectives are more specific than goals and more relatable to threats. **Purpose:** Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate definition of metrics or measures of effectiveness (MOEs). **Application:** Used in scoring methods or summaries of analyses (e.g., cyberresiliency posture assessments).
	Sub-Objective		**Definition:** A statement, subsidiary to a cyberresiliency objective, which emphasizes different aspects of that objective or identifies methods to achieve that objective. **Purpose:** Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. **Application:** Used in scoring methods or analyses; may be reflected in system functional requirements.
		Activity or Capability	**Definition:** A statement of a capability or action which supports the achievement of a sub-objective and, hence, of an objective. **Purpose:** Facilitate the definition of metrics or MOEs. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization. **Application:** Used in scoring methods or analyses; reflected in system functional requirements.

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Figure 4—Cyberresiliency Approaches

Techniques	Approaches	Examples
Adaptive Response Implement agile courses of action to manage risk factors.	**Dynamic Reconfiguration** Make changes to individual systems, system elements, components or sets of cyber resources to change functionality or behavior without interrupting service.	• Dynamically change router rules, access control lists, intrusion detection and prevention system parameters, and filter rules for firewalls and gateways. • Reassign cyberdefense responsibilities to personnel or operating centers.
	Dynamic Resource Allocation Change the allocation of resources to tasks or functions without terminating critical functions or processes.	• Employ dynamic provisioning. • Reprioritize messages or services. • Implement load-balancing. • Provide emergency shutoff capabilities. • Preempt communications.
	Adaptive Management Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment.	• Disable access dynamically. • Implement adaptive authentication. • Provide for automatic disabling of the system. • Provide dynamic deployment of new or replacement resources or capabilities.

Figure 4—Cyberresiliency Approaches *(cont.)*

Techniques	Approaches	Examples
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.	**Monitoring and damage assessment** Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity and to detect and assess damage from adversity.	• Use hardware fault detection. • Employ continuous diagnostics and mitigation (CDM) or other vulnerability scanning tools. • Deploy intrusion detection systems (IDSs) and other monitoring tools. • Use insider threat monitoring tools. • Perform telemetry analysis. • Detect malware beaconing. • Monitor open-source information for indicators of disclosure or compromise.
	Sensor fusion and analysis Fuse and analyze monitoring data and analysis results from different information sources or at different times together with externally provided threat intelligence.	• Enable organizationwide situational awareness. • Implement cross-organizational auditing. • Correlate data from different tools. • Fuse data from physical access control systems and information systems.
	Forensic and behavioral analysis Analyze adversary TTPs, including observed behavior as well as malware and other artifacts left behind by adverse events.	• Deploy an integrated team of forensic and malware analysts, developers, and operations personnel. • Use reverse engineering and other malware analysis tools.
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner.	**Calibrated defense in depth** Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value.	• Design for defense in depth. • Employ multiple, distinct authentication challenges over the course of a session to confirm identity. • Combine network and host-based intrusion detection. • Provide increasing levels of protection to access more sensitive or critical resources. • Conduct sensitivity and criticality analyses.
	Consistency analysis Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps.	• Employ unified identity and access management (IdAM) administration tools. • Analyze mission/business process flows and threads. • Employ privilege analysis tools to support an ongoing review of whether user privileges are assigned consistently. • Interpret attributes consistently. • Coordinate the planning, training and testing of incident response, contingency planning, etc. • Design for facilitating coordination and mutual support among safeguards.
	Orchestration Coordinate the ongoing behavior of mechanisms and processes at different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps.	• Coordinate incident handling with mission/business process continuity of operations and organizational processes. • Conduct coverage planning and management for sensors. • Use cyber playbooks.
	Self-challenge Affect mission/business processes or system elements adversely in a controlled manner to validate the effectiveness of protections and to enable proactive response and improvement.	• Hardware power-on self-test. • Conduct role-based training exercises. • Conduct penetration testing and red team exercises. • Test automated incident response. • Employ fault injection. • Conduct tabletop exercises.

Figure 4—Cyberresiliency Approaches *(cont.)*

Techniques	Approaches	Examples
Contextual awareness Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action.	**Dynamic resource awareness** Maintain current information about resources, status of resources, and resource connectivity.	• Maintain real-time integrated situational awareness.
	Dynamic threat awareness Maintain current information about threat actors, indicators, and potential, predicted, and observed adverse events.	• Track predicted or impending natural disasters. • Dynamically ingest incident and threat data. • Facilitate integrated situational awareness of threats.
	Mission dependency and status visualization Maintain current information about the status of missions or business functions, dependencies on resources, and the status of those resources with respect to threats.	• Construct a broad (mission/business functionwide, organizationwide) perspective.
Deception Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.	**Obfuscation** Hide, transform or otherwise obfuscate information from the adversary.	• Encrypt data at rest. • Encrypt transmitted data (e.g., using a virtual private network [VPN]). • Encrypt authenticators. • Conceal or randomize communications patterns. • Conceal the presence of system components on an internal network. • Mask, encrypt, hash or replace identifiers. • Obfuscate traffic via onion routing. • Apply chaffing to communications traffic. • Add a large amount of valid but useless information to a data store. • Perform encrypted processing.
	Disinformation Provide deliberately misleading information to adversaries.	• Post questions to a public forum based on false information about the system. • Create false ("canary") credentials and tokens (e.g., honeytokens).
	Misdirection Maintain deception resources or environments and direct adversary activities there.	• Establish and maintain honeypots, honeynets or decoy files. • Maintain a full-scale, all-encompassing deception environment.
	Tainting Embed covert capabilities in resources.	• Use beacon traps. • Employ internal network table cache poisoning (e.g., Domain Name System (DNS), Address Resolution Protocol (ARP)). • Include false entries or steganographic data in files to enable them to be found via open-source analysis.
Diversity Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.	**Architectural diversity** Use multiple sets of technical standards, different technologies, and different architectural patterns.	• Use auditing/logging systems on different OSs to acquire and store audit/logging data. • Apply different audit/logging regimes at different architectural layers. • Deploy diverse operating systems. • Support multiple protocol standards.
	Design diversity Use different designs to meet the same requirements or provide equivalent functionality.	• Employ N-version programming. • Employ mixed-signal design diversity (using both analog and digital signals). • Employ mixed-level design diversity (using both hardware and software implementations).
	Synthetic diversity Transform implementations of software to produce a variety of instances.	• Implement address space layout randomization. • Use randomizing compilers.
	Information diversity Provide information from different sources or transform information in different ways.	• Apply different analog-to-digital conversion methods to non-digitally-obtained data. • Use multiple data sources.
	Path diversity Provide multiple independent paths for command, control and communications.	• Establish alternate telecommunications services (e.g., ground-based circuits, satellite communications). • Employ alternate communications protocols. • Use out-of-band channels.
	Supply chain diversity Use multiple independent supply chains for critical components.	• Use a diverse set of suppliers.

Figure 4—Cyberresiliency Approaches *(cont.)*

Techniques	Approaches	Examples
Dynamic positioning Distribute and dynamically relocate functionality or system resources.	**Functional relocation of sensors** Relocate sensors or reallocate responsibility for specific sensing tasks to look for indicators of adverse events.	• Relocate (using virtualization) or reconfigure IDSs or IDS sensors.
	Functional relocation of cyberresources Change the location of cyberresources that provide functionality or information, either by moving the assets or by transferring functional responsibility.	• Change processing locations (e.g., switch to a virtual machine on a different physical component). • Change storage sites (e.g., switch to an alternate data store on a different storage area network).
	Asset mobility Securely move physical resources.	• Move a mobile device or system component (e.g., a router) from one room in a facility to another while monitoring its movement. • Move storage media securely from one room or facility to another room or facility. • Move a platform or vehicle to avoid collision or other physical harm, while retaining knowledge of its location.
	Fragmentation Fragment information and distribute it across multiple components.	• Implement fragmentation and partitioning for distributed databases.
	Distributed functionality Decompose a function or application into smaller functions and distribute those functions across multiple components.	• Architect applications so that constituent functions can be located on different system components.
Non-persistence Generate and retain resources as needed or for a limited time.	**Non-persistent information** Refresh information periodically, or generate information on demand and delete it when no longer needed.	• Delete high-value mission information after it is processed. • Off-load audit records to off-line storage. • Use one-time passwords or nonces.
	Non-persistent services Refresh services periodically, or generate services on demand and terminate services when no longer needed.	• Employ time-based or inactivity-based session termination. • Re-image components. • Refresh services using virtualization.
	Non-persistent connectivity Establish connections on demand, and terminate connections when no longer needed.	• Implement software-defined networking. • Employ time-based or inactivity-based network disconnection.
Privilege restriction Restrict privileges based on attributes of users and system elements as well as on environmental factors.	**Trust-based privilege management** Define, assign and maintain privileges associated with active entities based on established trust criteria consistent with principles of least privilege.	• Implement least privilege. • Employ time-based account restrictions.
	Attribute-based usage restriction Define, assign, maintain and apply usage restrictions on systems containing cyberresources based on the criticality of missions or business functions and other attributes (e.g., data sensitivity).	• Employ role-based access control (RBAC). • Employ attribute-based access control (ABAC). • Restrict the use of maintenance tools.
	Dynamic privileges Elevate or decrease privileges assigned to a user, process or service based on transient or contextual factors.	• Implement time-based adjustment to privileges due to status of mission or business tasks. • Employ dynamic account provisioning. • Disable privileges based on a determination that an individual or process is high-risk. • Implement dynamic revocation of access authorizations. • Implement dynamic association of attributes with cyberresources and active entities. • Implement dynamic credential binding.

Figure 4—Cyberresiliency Approaches *(cont.)*

Techniques	Approaches	Examples
Realignment Align system resources with current organizational mission or business function needs to reduce risk.	**Purposing** Ensure systems containing cyberresources are used consistently with mission or business function purposes and approved uses.	• Use whitelisting to prevent installation of such unapproved applications as games or peer-to-peer music sharing. • Use whitelisting to restrict communications to a specified set of addresses. • Ensure that privileged accounts are not used for nonprivileged functions.
	Offloading Offload supportive but nonessential functions to other systems or to an external provider that is better able to support the functions.	• Outsource nonessential services to a managed service provider. • Impose requirements on and perform oversight of external system services.
	Restriction Remove or disable unneeded functionality or connectivity, or add mechanisms to reduce the chance of vulnerability or failure.	• Configure the system to provide only essential capabilities. • Minimize nonsecurity functionality.
	Replacement Replace low-assurance or poorly understood implementations with more trustworthy implementations.	• Remove or replace unsupported system components to reduce risk.
	Specialization Modify the design of, augment, or configure critical cyberresources uniquely for the mission or business function to improve trustworthiness.	• Re-implement or custom develop critical components. • Develop custom system elements covertly. • Define and apply customized configurations.
Redundancy Provide multiple protected instances of critical resources.	**Protected backup and restore** Back up information and software (including configuration data and virtualized resources) in a way that protects its confidentiality, integrity and authenticity, and enable restoration in case of disruption or corruption.	• Retain previous baseline configurations. • Maintain and protect system level backup information (e.g., operating system, application software, system configuration data).
	Surplus capacity Maintain extra capacity for information storage, processing or communications.	• Maintain spare parts (i.e., system components). • Address surplus capacity in service level agreements with external systems.
	Replication Duplicate hardware, information, backups or functionality in multiple locations, and keep them synchronized.	• Provide alternate audit capability. • Maintain shadow database. • Maintain one or more alternate storage sites. • Maintain one or more alternate processing sites. • Maintain a redundant secondary system. • Provide alternative security mechanisms. • Implement a redundant name and address resolution service.
Segmentation Define and separate system elements based on criticality and trustworthiness.	**Predefined segmentation** Define enclaves, segments or other types of resource sets based on criticality and trustworthiness so that they can be protected separately and, if necessary, isolated.	• Use virtualization to maintain separate processing domains based on user privileges. • Use cryptographic separation for maintenance. • Partition application from system functionality. • Isolate security functions from nonsecurity functions. • Isolate security tools and capabilities using physical separation. • Isolate components based on mission or business function. • Separate subnets that connect to different security domains. In particular, provide a DMZ for Internet connectivity. • Employ system partitioning. • Employ process isolation. • Implement sandboxes and other confined environments. • Implement memory protection.
	Dynamic segmentation and isolation Change the configuration of enclaves or protected segments, or isolate resources while minimizing operational disruption.	• Implement dynamic isolation of components. • Implement software-defined networking and VPNs to define new enclaves. • Create a virtualized sandbox or detonation chamber for untrusted attachments or URLs.

Figure 4—Cyberresiliency Approaches *(cont.)*

Techniques	Approaches	Examples
Substantiated integrity Ascertain whether critical system elements have been corrupted.	**Integrity checks** Apply and validate checks of the integrity or quality of information, components or services.	• Use tamper-evident seals and anti-tamper coatings. • Use automated tools for data quality checking. • Use blockchain technology. • Use nonmodifiable executables. • Use polling techniques to identify potential damage. • Implement cryptographic hashes. • Employ information input validation. • Validate components as part of SCRM. • Employ integrity checking on external systems.
	Provenance tracking Identify and track the provenance of data, software or hardware elements.	• Employ component traceability as part of Supply Chain Risk Management (SCRM). • Employ provenance tracking as part of SCRM. • Implement anti-counterfeit protections. • Implement trusted path. • Implement code signing.
	Behavior validation Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).	• Employ detonation chambers. • Implement function verification. • Verify boot process integrity. • Implement fault injection to observe potential anomalies in error handling.
Unpredictability Make changes randomly or unpredictably.	**Temporal unpredictability** Change behavior or state at times that are determined randomly or by complex functions.	• Require re-authentication at random intervals. • Perform routine actions at different times of day.
	Contextual unpredictability Change behavior or state in ways that are determined randomly or by complex functions.	• Rotate roles and responsibilities. • Implement random channel-hopping.

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

The NIST approach is more threat based. Every organization faces different internal and external threats depending on the nature of the organization and its processes. By using a threat-based approach to identify mitigating controls and business objectives, the organization develops an inventory of use cases to mitigate these threats using a prioritized approach. The organization must develop an inventory of use cases for cyberresilience that is applied to business processes, perhaps initially addressing the critical ones such as applications and supporting assets and the infrastructure supporting the business objectives. It is necessary to identify the gaps on a continual basis and continue to improve the process.

Example Checklist for Reviewing Cyberresilience Based on NIST 800-160

NIST 800-160 provides design principles that can be used to measure the cyberresilience of an organization (**figure 5**). Again, any strategic design principles are driven by an organization’s risk management strategy and its risk framing. In this case, developing and fine-tuning a risk management strategy includes identifying the assumptions and dependencies, threats and overall risk that impact the organization, its customer data and organizational priorities.

Figure 5—Strategic Cyberresiliency Design Principles

Strategic Design Principles	Key Ideas	Related Design Principles From Other Disciplines
Focus on common critical assets.	Limited organizational and programmatic resources need to be applied where they can provide the greatest benefit. This results in a strategy of focusing first on assets which are both critical and common, then on those which are either critical or common.	**Security:** Inverse modification threshold **Resilience Engineering:** Physical redundancy, layered defense, loose coupling **Survivability:** Failure mode reduction, fail-safe, evolution
Support agility and architect for adaptability.	Not only does the threat landscape change as adversaries evolve, so do technologies and the ways in which individuals and organizations use them. Both agility and adaptability are integral to the risk management strategy in response to the risk framing assumption that unforeseen changes will occur in the threat, technical, and operational environment through a system's lifespan.	**Security:** Secure evolvability, minimized sharing, reduced complexity **Resilience Engineering:** Reorganization, human backup, inter-node interaction **Survivability:** Mobility, evolution
Reduce attack surfaces.	A large attack surface is difficult to defend, requiring ongoing effort to monitor, analyze and respond to anomalies. Reducing attack surfaces decreases ongoing protection scope costs and makes the adversary concentrate efforts on a small set of locations, resources or environments that can be more effectively monitored and defended.	**Security:** Least common mechanism, minimized sharing, reduced complexity, minimized security elements, least privilege, predicate permission **Resilience Engineering:** Complexity avoidance, drift correction **Survivability:** Prevention, failure mode reduction
Assume compromised resources.	Systems and system components, ranging from chips to software modules to running services, can be compromised for extended periods without detection. In fact, some compromises may never be detected. Systems must remain capable of meeting performance and quality requirements, nonetheless.	**Security:** Trusted components, self-reliant trustworthiness, trusted communications channels. *Incompatible with security:* hierarchical protection **Resilience Engineering:** Human backup, localized capacity, loose coupling
Expect adversaries to evolve.	Advanced cyberadversaries invest time, effort, and intelligence-gathering to improve existing and develop new tactics, techniques and procedures (TTPs). Adversaries evolve in response to opportunities offered by new technologies or uses of technology, as well as to the knowledge they gain about defender TTPs. In (increasingly short) time, the tools developed by advanced adversaries become available to less sophisticated adversaries. Therefore, systems and missions need to be resilient in the face of unexpected attacks.	**Security:** Trusted communications channels **Resilience Engineering:** Reorganization, drift correction **Survivability:** Evolution

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Figure 6—Tailorable Process for Cyberresiliency Analysis

Analysis Step	Motivating Question	Tasks
Understand the context.	How do stakeholder concerns and priorities translate into cyberresiliency constructs and priorities?	• Identify the programmatic context. • Identify the architectural context. • Identify the operational context. • Identify the threat context. • Interpret and prioritize cyberresiliency constructs.
Establish the initial cyber resiliency baseline.	How well is the system doing—how well does it meet stakeholder needs and address stakeholder concerns—with respect to the aspects of cyberresiliency that matter to stakeholders?	• Identify existing capabilities. • Identify gaps and issues. • Define evaluation criteria and make initial assessment.
Analyze the system.	How do cyberrisk factors affect mission, business or operational risk?	• Identify critical resources, sources of fragility and attack surfaces. • Represent the adversary perspective. • Identify and prioritize opportunities for improvement.
Define and analyze specific alternatives.	How can mission or operational resilience be improved by improving cyberresiliency?	• Define potential technical and procedural solutions. • Define potential solutions for supporting systems and processes. • Analyze potential solutions with respect to criteria.
Develop recommendations.	What is the recommended plan of action?	• Identify and analyze alternatives. • Assess alternatives. • Recommend a plan of action.

Source: National Institute of Standards and Technology (NIST), SP 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

Cyberresilient examples are illustrated in **figure 6**.

Operational Checklist

Using the NIST guidance, the checklist illustrated in **figure 7** can be operationalized to review an organization's cyberresilience approach for completeness and overall robustness.

Applying the Concept of Cyberresilience or the NIST Model

There are four steps organizations can take to strengthen their operational resilience programs:

1. Review the organization's operational resilience program to understand how the program compares to regulatory requirements (e.g., Bank of England,[10] US Federal Financial Institutions Examination Council [FFIEC][11]), industry standards (Disaster Recovery Institute International [DRII],[12] International Organization for Standardization [ISO] ISO 22301[13]) and generally accepted best practices. The creation and maintenance of a regulatory book of record, along with periodic assessments against those requirements, supports proper oversight controls.
2. Create a scenario library of severe but plausible disruptions, threats and events. This may include a mix of natural, man-made, third-party, human capital and technology threats. Within technology threats, cyberattack threats such as malware, phishing, distributed denial of service (DDoS) and ransomware should be included.
3. Validate the organization's operational resilience program against the previously identified threat scenario library. Validation will be considered sufficient if testing is

Figure 7—Cyberresilience Completeness Checklist

Technique	Approach	Description	Threat Use Case (MITRE Framework)	Assumptions	Cyber Resilience Approach
Adaptive Response Implement agile courses of action to manage risks.	**Dynamic Reconfiguration**	Make changes to individual systems, system elements, components, or sets of cyberresources to change functionality or behavior without interrupting service.	Privileged escalation	Operation system logs are available to enable the enterprise to be resilient	Implement trust-based privileged management.
				Change control process. Ensure that systems undergoing patching remain capable of meeting performance and quality requirements through loose coupling.	Implement attribute-based usage restriction to make system, device or other application changes.
				Persistence	Explore dynamic provisioning implement multifactor authentication where possible.
			APT	Access to sensitive data is not restricted using a maturity model	1. Constant monitoring of critical assets. 2. Coordinate architecture of Firewall, WAF and AV, IPSIDS. 3. Force unauthorized users to a sandbox. 4. Utilize a VPN. 5. Email encryption. 6. Use of MSSO. 7. Patch regularly. 8. Use multifactor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access a critical (sensitive high-availability) data repository. Do daily backups of important newly changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. 9. Review system and OS configuration updates. 10. Avoid plan for loss of data. 11. Include privacy at every stage in development of processes or products.

Figure 7—Cyberresilience Completeness Checklist *(cont.)*

Mitigation to Reduce Attack Surface	Focus on Common Critical Asset	Expect Adversaries to Evolve	Steps	Description
Remove users from the local administrators on systems: 1. Implement privileged users based on “least privilege.” 2. Predicate permission to these accounts.	Focus on high-value enterprise assets, risk ranked using an approved risk framework, based on nonpublic information, ability to commit fraud, etc.	Evolve the process.	Dynamically change router rules, access control lists, intrusion detection and prevention system parameters, and filter rules for firewalls and gateways	
Check for common UAC bypass weaknesses on Windows system to be aware of the risk posture and address issues where appropriate: 1. Implement privileged users based on “least privilege.” 2. Predicate permission to these accounts, 3. Reduce complexity of change process		Make system resilient in the face of unexpected attacks through evolution.	Reassign cyber defense responsibilities to personnel or operating center.	
Implement profile to customize user logons or their environment. MITRE indicates “an administrator can also configure a profile that applies to all users and host programs or the local computer.”		1. Use trusted communications channels in the enterprise where possible. 2. Reorganize if applicable. 3. More attention by monitoring to audit trails of critical systems and key accounts. 4. Become more aware of knowledge others may have about enterprise TTPs within cybersecurity. 5. Attempt to disguise tools, techniques and access data such as using honeypots. 6. Leverage tools and their use	• Disable access dynamically. • Implement adaptive authentication. • Employ dynamic provisioning. • Implement load-balance. • Provide emergency shutoff capabilities. • Provide for automatic disabling of the system. • Provide dynamic deployment of new or replacement resources or capabilities.	Adversaries may gain persistence and elevate privileges in certain situations by abusing PowerShell profiles. A PowerShell profile (profile.ps1) is a script that runs when PowerShell starts and can be used as a logon script to customize user environments. PowerShell supports several profiles depending on the user or host program. For example, there can be different profiles for PowerShell host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administration can also configure a profile that applies to all users and host programs on the local computer.
1. Use application whitelisting to help prevent malicious software and unapproved programs from running. 2. Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office. 3. Patch operating system vulnerabilities. 4. Restrict administrative privileges to operating systems and application, based on user duties.				

Source: *https://encylopedia.kaspersky,com/knowledge/sstrategies-for-mitigating-advanced-persistent-threats-aps*

successful and processes can be reestablished within prescribed recovery time objectives.

4. Initiate a continuous feedback loop. Once a test is completed for a given scenario, the necessary program improvements should be made and then testing should begin against a new scenario. Testing should evolve along a maturity matrix with each subsequent test increasing in complexity and rigor. In addition, testing categories should be revisited on a regular cadence to ensure a state of readiness against a broad range of threats.

Conclusion

Cyberresilience is a relatively new term, but it requires organizations to apply basic common sense to their controls to mitigate threats, whether external or internal, using a thought-based

> THE CREATION AND MAINTENANCE OF A REGULATORY BOOK OF RECORD, ALONG WITH PERIODIC ASSESSMENTS AGAINST THOSE REQUIREMENTS, SUPPORTS PROPER OVERSIGHT CONTROLS.

approach. NIST guidance provides risk-based approaches and a framework that can be an important tool for organizations to improve their cyberresiliency.

Endnotes

[1] US Chamber of Congress, *Internet Security Essentials for Business 2.0*, USA, October 2012, *https://www.uschamber.com/CybersecurityEssentials*

[2] Ross, R.; V. Pillitteri; R. Graubart; D. Bodeau; R. McQuaid; Special Publication (SP) 800-160 vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, National Institute of Standards and Technology (NIST), USA, November 2019, *https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final*

[3] Forcepoint, "What Is Defense in Depth?" *https://www.forcepoint.com/cyber-edu/defense-depth*

[4] *Ibid.*

[5] ManageEngine ServiceDesk Plus, "What Is ITIL Incident Management?" 25 June 2020, *https://www.manageengine.com/products/service-desk/itil-incident-management-guide.html*

[6] ISACA®, *IT Contingency Planning Audit Program*, USA, 2009, *https://www.isaca.org/bookstore/it-governance-and-business-management/wapcp*

[7] *Op cit* Ross

[8] (ISC)^2, *(ISC)^2 Cybersecurity Workforce Study, 2019: Strategies for Building and Growing Strong Cybersecurity Teams*, USA, 2019, *https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019*

[9] *Ibid.*

[10] Bank of England, *Operational Resilience: Impact Tolerances for Important Business Services*, United Kingdom, 5 December 2019, *https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper*

[11] Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook Infobase, *Business Continuity Management*, USA, *https://ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx*

[12] Disaster Recovery Institute International (DRII), *https://drii.org/*

[13] International Organization for Standardization (ISO), ISO 22301:2019 *Security and Resilience—Business Continuity Management Systems—Requirements*, Switzerland, 2019, *https://www.iso.org/standard/75106.html*