DREW
Blandford-Williams

GRC

cybersecurity consulting services

Cyber*Defense*

The Business of Protecting ***'the Business'***

Understanding the Modified NIST Risk Management Framework

Cyber-Defense

The Business of Protecting
'the Business'

While it's true, an organization cannot prevent a security event from happening, there are some practical steps you can take to reduce your threat exposure while also manage the potential impact of an event in your environment. The MSSP has a few suggestions to help you improve your security posture.

Not "If" But "When" You Are Compromised

It's not a matter of "If" your organization will be compromised, it's a matter of how prepared you will be and how fast you can **identify**, **respond** to, **contain** and **recover** from security event.

Although there are many ways in which a system might be compromised, and as a trusted partner and Managed Service Provider, The MSSP recommends you consider the following actions as a good starting point to improving cybersecurity maturity within your operations.

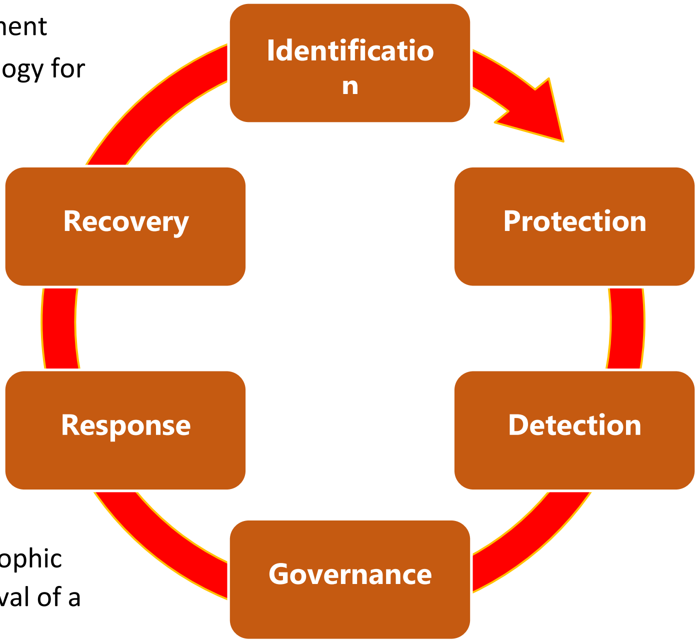
The first order of business is to ensure that your organization has at least a fundamental agreement on how to manage "Security" issues, which usually translates into a combination of tools and processes with executive oversight and governance. Any operation that includes managing or accessing sensitive data needs ***The MSSP's Modified NIST Risk Management Framework Services***.

This complete suite of professional and managed security services provides laser-focused security deterrence capabilities, which enable your business to improve its cybersecurity posture and defend its assets from threat of compromise.

The six phases of The MSSP Risk Management Framework provide a repeatable methodology for applying critical care and security focus to controls and processes that are essential to conducting business operations.

The six phases—Identification, Protection, Detection, Governance, Response, and Recovery—provide a balanced approach to implementing and managing proactive safeguards to address and contain a cyber incident.

This balance is especially important in mid-enterprise market sectors in which worst-case incidents could result in catastrophic impact to the integrity and long-term survival of a business.



Starting with a Proven Risk Management Framework

The MSSP Risk Management Framework considers all six functions that a Cyber-*Defense* strategy must include to improve the security maturity and defensive posture of any organization, and help them reduce their *attack footprint*:

1. **Identification**
   Organizations must develop an understanding of their environment to manage cybersecurity risk to systems, assets, data and capabilities. Attaining full visibility into your digital and physical assets and their interconnections, defined roles and responsibilities, are fundamental to understanding the types of risks you may be exposed to, while also allowing you to target specific policies and procedures to consider as part of managing those risks.

   - Identifying the business environment your organization supports including its role in the supply chain.
   - Identifying cybersecurity policies your business currently has established as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities to which your business sector may align.
   - Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for a Risk Assessment plan.

2. **Protection**
   The Protection impact point outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Developing and implementing appropriate safeguards to limit or contain the impact of a potential cybersecurity event are essential tenets of the Protection phase. To comply, your organization must control access to digital and physical assets, provide awareness education and training, put processes into place to secure data, maintain baselines of network configuration and operations to repair system components in a timely manner and deploy protective technology to ensure cyber resilience. Protections should include as fundamental tenets:

- Empowering your staff through Awareness and Training including role-based and privileged user training.
- Establishing Data Security protection consistent with your organization's risk strategy to protect the confidentiality, integrity, and availability of data.
- Implementing Information Protection *Processes and Procedures* to maintain and manage the protections of information systems and assets.

3. **Detection**

Detection defines the appropriate activities to identify the occurrence of a cybersecurity event and contain the event based on *Indicators of Compromise* ("IOC"). To remain in a constant cyber-defensive posture, your business needs to implement appropriate measures to quickly identify and contain cybersecurity events. The adoption of continuous monitoring solutions that detect anomalous activity and other threats are core competencies associated with this phase.

Your organization must have visibility into its networks to anticipate a cyber incident and can respond and defend as needed, and at a minimum:

- Ensure Anomalies and Events are detected, and their potential impact is understood.
- Implement Security Continuous Monitoring capabilities to monitor cybersecurity events and verify the effectiveness of protective measures including network and physical activities.
- Maintain Detection/Mitigation Processes to provide awareness of anomalous events.

4. **Governance**

Information Security Governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to ensure that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

The purpose of information security governance is to ensure that your organization is proactively implementing appropriate information security controls to support its mission in a cost-effective manner, while managing evolving information security risks. As such, information security governance has its own set of requirements, challenges, activities, and types of possible structures.

Governance also has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities.

5. **Response**

The Response phase includes activities to take follow-up action specific to detecting and containing a known event, and supports the ability to contain the impact of a potential cybersecurity incident ahead of a potential compromise.

Should a cyber incident occur, your business needs to have the ability to contain the impact. To address this phase of the cycle, an organization needs to collect and analyze information about the event, perform all required activities to eradicate the incident and incorporate lessons learned into revised response strategies. At a minimum, Response solutions should:

- Ensure Response Planning process are executed during and after an incident.
- Analyze the evidence to determine impact and to ensure effective response and support recovery activities including forensic analysis.
- Perform mitigation activities to prevent expansion of an event and to resolve the incident.
- The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities and feeds that knowledge back into their respective controls, processes and system configurations.

6. **Recovery**

The Recovery phase identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were compromised due to a cybersecurity incident. Recovery also supports timely restoration of normal operations to reduce the impact from a cybersecurity incident.

Recovery plans can be as elaborate as the businesses that govern them, but they can also be as simple as identifying who to call in case of an emergency. Your organization should have a recovery plan in place, be able to coordinate restoration activities with external parties and incorporate lessons learned into your updated recovery strategy. And in some cases, in which external mandates, such as the GDPR, CCPA, HIPAA and PCI are in effect, a Recovery plan of some type is required to comply with the rule.

Defining a prioritized list of action points which can be used to undertake recovery activity is critical for a timely recovery, and should include:

- Ensuring your business implements Recovery Planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents.
- Implementing Improvements based on lessons learned and reviews of existing strategies.

Where should we begin building our defenses?

Understanding the threat landscape assists our customers in making informed risk management decisions that will result in a greater defensive posture, while also allowing organizations to protect areas that matter most to achieving business goals.

1. How does "Risk" ***Impact*** C-I-A within business operating environment and your respective customers' own environments?
2. Is the information relating to the risk ***Timely***?
3. How ***Relevant*** is the information we are collecting about the potential compromise?
4. Can or is the attack/threat populating like a virus (i.e., "***Replicating***")?
5. What is the order of ***Priority*** for addressing market drivers, client needs and business expansion?

The MSSP RMF Maps Security Solutions to Defend your System

The MSSP's Modified NIST Risk Management Framework (RMF) Services can be used by businesses that already have extensive cybersecurity programs as well as by those just considering using cybersecurity management programs. This portfolio of services follows a series of processes that your organization may integrate into its operations to reduce its attack surface.

These services were designed based on three points of reference: Relevance, Timeliness and Impact of a risk.

Identification

- ***Security Diagnostics Assessment Services***
  The MSSP's Security Analyst service is designed to be an addon to existing The MSSP contracts. It is delivered in the form of a pre-agreed upon bucket of monthly dedicated hours.

- ***Vulnerability Management Services***
  n the digital age, regardless of your organization's size, there is a persistent cyber threat, but in the cybersecurity landscape, you do not need the highest security possible, you just need to be slightly more secure than industry standard. A strong security program activates best security practices upon understanding an organization's needs, culture, and business operations.

- ***Threat Assessment Services***
  A strong security program is cultivated by understanding an organization's needs, culture, and business operations. The MSSP Managed Security Services Suite provides a blended approach to ensure that security processes are a prioritized, highly focused set of action items and not just another item on the to do list. Once the diagnostics are complete, The MSSP can provide a skilled support network to implement the security measures scaled to your company, compliant with all industry or government security requirements.

2. **Protection**

   - ***Endpoint Protection as a Service***
     The MSSP's Endpoint Protection Service (EPaaS), provides customers with the endpoint protection needed to navigate today's threat landscape with minimal interruptions. The MSSP is continuously evaluating security vendors who are best suited to protect your endpoints, so you don't have to.

3. **Detection**

   - ***SOC as a Service***
     The MSSP's Secure Operations Center Services (SOC as a Service), provide organizations all the benefits needed from a security information and event management system without any of the headache or capital investment. The offering is a comprehensive SOCaaS solution, fully hosted in a secure and compliant cloud to manage and monitor your critical systems regardless of where they may be.

   - ***Network Anomaly & Ransomware Defense Services***
     Ransomware has become the most prominent and malicious type of malware. While attackers used to steal information to use against target sites, these attackers did not typically hold systems at bay, or worse—destroy them.

4. **Governance**

   - ***^{V}CISO Augmentation Services***
     Virtual CISO Consulting Services provides your company with a senior executive that is well versed in risk management and possesses a strong background in IT leadership. The vCISO engages with your organization on a regular basis to define and implement security, compliance, governance policies and procedures.

   - ***Data Privacy Impact Assessment Services***
     Data privacy regulations, like the GDPR and CCPA, require data privacy to be considered before implementing a project or a process that may impact the integrity of protected information.

     The MSSP provides Data Privacy Impact Assessments based first on the criteria as defined by the GDPR and CCPA.

5. **Response**

   - ***Incident Response & Event Orientation***
     Data breaches aren't always the result of a malicious hacker. In fact, most of the time, the loss originates from an unsuspecting operation performed by an employee. Data is also constantly at risk with natural disasters and inconsistent system updates. In today's Digital world, it's not about when you are compromised, it's about controlling how much data is lost and getting back to work!

6. **Recovery**

    - ***Business Continuity / Disaster Recovery***
      Through our ongoing Program and Project Management Services, we build a continuous pipeline of feedback and improvement; our Project stakeholders never lose sight of progress and propagate a culture of collective success that embraces change every day. We ensure your project is on track and focus on getting a commitment from ownership while maintaining accountability from teams for key milestones.