Why A Need For Increased Cybersecurity Hygiene?

Thirty years of history have shown that cyber risk is difficult to understand, problematic to hedge, only likely to increase, and characterized by a continually changing threat environment. Tomorrows cyberattacks may not look much like today's — as evidenced by 2023's spate of ransomware compared to the previous breaches. The cyber landscape is constantly evolving, resulting in a significant increase in coverage costs highlighted by the following six reasons: 1. Ransomware; 2. Rising Response Costs; 3. Increasing Replacement Costs; 4. Inadequate Cybersecurity Hygiene; 5. Lack of Incident Response Plans; and 6. Business Interruption. Until then, businesses will need to increase their ***Cybersecurity Hygiene*** – highlighted by implementing cybersecurity processes, tools, information sharing, playbooks, exercises, and training with end-goal of enhancing the protection of their critical data and systems – **reducing our risk.**

In the next five phases, we'll explore the five key components of a sound cybersecurity foundation, a Cybersecurity Plan, based on the NIST Cybersecurity Framework and we'll cover industry best practices and solutions like risk management, incident response (IR) planning and managed detection and response (MDR) – tools you can use to build out an effective, practical threat management strategy.

Essentially Cyber Hygiene is like any kind of hygiene, it's the daily practice of taking care of those things that could deteriorate over time if not given the proper attention, like brushing your teeth twice a day-fundamental practice of maintaining a healthy security environment. Some of the practices may include proper inventory of software and hardware assets, continuous scanning of system vulnerabilities, etc. To increase Cybersecurity Hygiene, our Framework addresses five (5) functional areas consisting of:

a. **Identify** - What processes and assets need protection?
b. **Protect** - What safeguards are available?
c. **Detect** - What techniques can be used to identify incidents?
d. **Respond** - What techniques can be used to contain impacts of incidents and mitigate?
e. **Recover** - What techniques can restore capabilities?

Protecting your organization is an ongoing process, a layered approach, and it requires careful planning. But with the right people, technology, policies, and governance in place, you're more likely to find and fix vulnerabilities, detect, and thwart threats and avert disaster. Getting there isn't necessarily easy, but you don't have to do it alone. Our Cyber Hygiene Roadmap can help you cut through the clutter, complexity, and confusion.

Phase 1: Identify - What processes and assets need protection?

You can't protect what you can't see, and the first step in the threat management lifecycle is about making sure you see into every corner of your organization. You'll identify your assets, their risks and vulnerabilities, their priority levels and, finally, your specific plans to protect them. Before you can begin to make those plans, you must know what apps you're running and on what devices, how your network is structured, what data you're using and storing and how your users are accessing it all. You must know the risks associated with each asset and prioritize those assets so you can manage risks accordingly.

ROADMAP:

- ○ Identify your assets, including data, devices, cloud and on-premises infrastructure, software, and networks, by conducting a comprehensive inventory. Prioritize assets or asset groups based on business value.
- ○ Determine and document your cybersecurity policies and procedures for operations, backup and recovery / business continuity, risk management and compliance. These documents should include your cadences for

routine threat management activities such as backups, vulnerability scans, updates and patches, and training.

- ○ Set identity access management (IAM) policies across all assets, then remove unauthorized devices, systems, software, and users from the network.
- ○ Find the attack surfaces and specific risks in your environment by conducting a comprehensive vulnerability assessment, including penetration testing.
- ○ Develop and test incident response plans that include step-by-step instructions for handling different incidents and types of attacks based on your specific environment.
- ○ To increase Cybersecurity Hygiene, develop a Cybersecurity Plan that is built upon the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is aligned to the DHS Nationwide Cybersecurity Review (NCSR) (https://www.cisecurity.org/ms-isac/services/ncsr) assessment methodology which addresses five (5) functional areas (Identify, Protect, Detect, Respond, and Recover)

The success of your cybersecurity strategy relies on comprehensive proacting planning and testing. The objective expertise of a third-party vendor can be valuable at this stage, especially when it comes to uncovering your blind spots. Consider exploring your options for risk management, internal and external security testing, compliance consulting and virtual CISO (vCISO) services.

Phase 2: Protect - What safeguards are available?

Protecting your organization is an ongoing and multi-threaded effort. Taking a risk-based approach is key to bringing your routine threat management activities to life, as documented in your Cybersecurity Plan highlighted by cybersecurity policies and procedures.

ROADMAP:

- ○ Develop, implement, or revise, and test Cybersecurity Plan, including cyber incident response plans, with clearly defined roles and responsibilities.
- ○ Implement IAM controls based on the principles of least privilege and separation of duties. Review these controls quarterly.
- ○ Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.
- ○ Configure systems, software, and devices for security, implementing built-in safeguards such as firewalls, data encryption and multi-factor authentication. Apply uniform configurations to like devices and disable unnecessary features.
- ○ Implement enhanced logging.
- ○ Data encryption for data at rest and in transit.
- ○ Limit End use of unsupported/end of life software and hardware that are accessible from the Internet.
- ○ Prohibit use of known/fixed/default passwords and credentials.
- ○ Ensure the ability to reconstitute systems (backups).

- ○ Equip and monitor every endpoint device with effective and up-to-date antivirus software.
- ○ Create regular secure backups on a frequency consistent with your recovery time and recovery point objectives.
- ○ Update your asset inventory monthly.
- ○ Conduct routine vulnerability scanning, with weekly vulnerability threat feeds, monthly external scanning, quarterly internal scanning, and annual penetration testing.
- ○ Keep systems and software updated and patched based on vulnerability scan results and as directed by vendors.
- ○ Routinely test and update your backup and recovery mechanisms as well as your business continuity plan.
- ○ Review, Coordinate, Develop, Publish and Maintain Cybersecurity Policies on a Cybersecurity Portal – Recommended policies consist of:

    1) Vulnerability Scanning Policy
    2) Penetration Testing Policy
    3) Social Engineering Policy
    4) Email Spam Filters Policy
    5) Network Firewall Policy
    6) Security GAP Assessment Template
    7) Security Operations Center (SOC) Strategy
    8) Managed Security Services Strategy
    9) Intrusion Detection And/Or Prevention Systems Policy
    10) SIEM Solution Strategy
    11) Workstation Policy
    12) Acceptable Use Policy
    13) Clean Desk Policy
    14) Remote Access Policy
    15) VPN Policy
    16) Teleconferencing (Zoom, MS Teams, etc.) Policies
    17) AI Policy
    18) Operational Technology (OT) Policy

- ○ Provide foundational cybersecurity awareness training to all employees, followed by refresher training, and phish testing on an ongoing basis to keep cybersecurity top of mind.
- ○ Ensure your agency has awareness and participates in a limited number of free services offered by CISA/OHS.
- ○ Ensure your agency participates annually in the NCSR, which is a free, anonymous, annual self-assessment
- ○ Ensure your agency subscribes to the Missouri Office of Homeland Security (OHS) Cybersecurity Program and participates in information sharing with federal, state, and local agencies such as Missouri Office of Homeland Security (OHS), Missouri Information Analysis Center (MIAC), St. Louis, Fusion Center, Kansas City Regional Fusion Center), and MCCoE.
- ○ Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).
- ○ Update Cybersecurity Plan.

For some organizations, these ongoing action items are more than can be managed with in-house resources. Despite best efforts, critical activities can fall through the cracks, leaving gaps in your cybersecurity strategy. As a result, businesses of all sizes often turn to security services providers to augment the capabilities and capacity of the security team. Consider outsourcing security testing and controls validation activities such as penetration testing, vulnerability management and application security testing.

Phase 3: Detect - What techniques can be used to identify incidents?

Organizations with even the strongest security controls can be compromised, but the faster a security incident can be identified and contained, the lower the costs associated with it. Bad actors such as ransomware groups can have your systems encrypted within an hour of gaining entry.5 That's why detecting incidents as soon as possible is crucial. Unfortunately, it can take months to detect and contain a breach. According to the 2021 IBM Cost of a Data Breach report, it takes 287 days on average – 212 days to identify a breach and another 75 days to contain it. A breach with a lifecycle over 200 days costs an average of $4.87 million versus $3.61 million for one with a lifecycle of less than 200 days, representing a difference of almost 30%. The differences in impact are substantial when you can detect and contain a threat in minutes versus hours, days or even months. According to recent research, smaller organizations are less likely to detect breaches in a timely manner than larger ones. Regardless of the size of the organization, 80% of breaches are discovered by external parties, a number that clearly indicates the need for organizations to put more emphasis on threat detection and response operations.

ROADMAP:

- ○ Maintain full visibility into data, devices, logs, cloud-based and on-premises systems infrastructure, software, and networks.
- ○ Implement 24/7 monitoring for threats and incidents across all environments.
- ○ Know how data normally flows through your organization. Deploying a network sensor can help, alerting you when data is suddenly flowing in an unexpected direction/path—a strong indicator that something could be amiss.
- ○ Maintain and monitor logs that record events such as IAM activity, changes to systems or accounts and the initiation of communication channels.
- ○ Deploy security tools such as security information and event management (SIEM) that can aggregate these logs and look for deviations from expected network behavior.
- ○ Consider implementing other security tools such as endpoint detection and response (EDR), file integrity monitoring (FIM) and intrusion detection system (IDS).
- ○ Consider implementing next-generation firewalls, which can provide in-depth information such as deep packet inspection as well as intrusion prevention capabilities.
- ○ Separate real incidents from the noise of alerts so you can prioritize anomalies for investigation. Fine-tuning your SIEM can help reduce false positives, resulting in a more manageable volume of alerts to investigate.
- ○ Test and tune your detection mechanisms on a regular basis.
- ○ Conduct Annual Penetration Test and Assessments.
- ○ Review and Update Cybersecurity Strategy Plan.

Phase 4: Respond - What techniques can be used to contain impacts of incidents and mitigate?

When a breach happens, it's critical to have an incident response plan in place that can immediately guide you through each stage of response. During an incident is not the time for determining your policy on paying a ransom or identifying your key stakeholders. That's what your incident response plan, discussed in Phase 1, is for. Your incident response plan is not a one-and-done exercise. It's a living document that must be tested and updated regularly. Each person must understand their role and responsibilities in order for your organization to respond effectively. It's also not a one-size-fits-all document. Your planned response to ransomware will be different than your response to a data breach, which will be different than your response to a lost or stolen device. Your incident response plan should include different playbooks to reflect different potential risks and scenarios. It should also reflect different potential threat vectors. Malicious data breaches occur through a wide range of threat vectors, including compromised credentials, cloud misconfigurations, vulnerabilities in third-party software and phishing. In fact, according to IBM research, those vectors account for nearly 75% of all malicious data breaches.

It often makes sense for an organization to seek outside expertise at this point in order to minimize the damage of an attack. Having access to SOC and incident response capabilities can dramatically shorten your mitigation and recovery time. Ideally, you've engaged an MDR provider that can move seamlessly into incident response when the time comes.

ROADMAP:

- ○ Review the security event to confirm it's not a false positive and then work quickly to triage the incident to investigate the type and source of the attack and assess the potential scope of the impact.
- ○ Stop the incident immediately to reduce the impact on business operations. Contain the threat by isolating or shutting down the affected systems, networks, servers, databases, and devices to prevent further spread to your network.
- ○ Preserve evidence and collect critical information while it's still available. Gather logs, memory dumps, audits, network traffic reports and disk images – any evidence that can be used to analyze the origin, impact, and intention behind the attack.
- ○ Eradicate the threat and prevent future occurrence. Patch the entry point to ensure the attacker cannot regain access.
- ○ Determine if any sensitive information was breached or data loss occurred.
- ○ Initiate communications with internal and external stakeholders, as outlined in your incident response plan. Work with your communications team on the content and timing of public statements.
- ○ Engage with your legal team and examine any compliance or regulatory risks to determine potential violations. Contact law enforcement and any other required government agencies.
- ○ Perform a root cause analysis to determine the attacker's steps to gain access to your systems and update protection and detection mechanisms accordingly.
- ○ Perform a company-wide vulnerability analysis to ensure all vulnerabilities have been addressed.
- ○ Keep a log of all incident response activities and results of investigations.
- ○ Update Cybersecurity Plan.

Phase 5: Recover - What techniques can restore capabilities?

The goal of recovery is to move from the immediate aftermath of an incident to full restoration of normal systems and operations," says the National Cybersecurity Alliance. Like all of the other components of the threat

management strategy, it requires thoughtful planning to fully restore normal systems and operations. Recovery often begins immediately on the heels of – or overlaps with – incident response.

ROADMAP:

- ○ Confirm that all the necessary forensic evidence has been collected.
- ○ Fully restore normal systems and operations. Repair, restore or replace affected components, whether that means restoring system images, restoring data from backups, or replacing potentially compromised controls such as passwords or encryption keys.
- ○ Leverage evidence and other critical information collected during the incident for post-incident analysis and reporting. Discuss the effectiveness of the incident response plan and adjust accordingly.
- ○ Capture lessons learned that would reduce the risk of a future incident, minimize the severity of a future incident, or improve incident response time. Incorporate these improvements into your policies and procedures for operations, backup and recovery / business continuity, risk management and compliance.
- ○ Organization to establish cyber workforce development & training plans, based on the NICE Cybersecurity Workforce Framework.
- ○ Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.
- ○ Update employee training and the incident response plan accordingly and communicate these updates to all stakeholders.
- ○ Update Cybersecurity Plan.

About the MCCoE

MCCoE - Located in the Jordan Valley Innovation Center (JVIC), Springfield, MO

The Missouri Cybersecurity Center of Excellence (MCCoE) is a non-profit (501.c.3), **Public-Private Partnership between Academia, Industry, Non-Profits and Government**, security operations center that brings together academia, small to medium sized businesses, government agencies, and the community. The MCCoE provides security services for businesses and agencies utilizing the skills and knowledge of the key cybersecurity professionals, professors, and students. By providing a rich and interactive learning environment, we build the next generation of cybersecurity professionals, connect the right people to the right careers, and close the gap in demand for these professionals in the State of Missouri regional workplace. By capitalizing on Missouri's unique strengths in this expanding and future-oriented field of cybersecurity, the MCCoE, based in Springfield, aims to create "career ready" students while growing the regional economy by providing Cybersecurity Services to the regional community strategically teamed with the regional colleges and universities to provide hands-on training, certifications and real-work experiences and accelerated innovation, while creating workforce development combined with a coordinated and collaborative cybersecurity strategy to strengthen our Region, our State, and our Nation.

Visit www.MCCoE.com for more information.