VITAL CYBER
Provided by MCNC

Blog Series- Cybersecurity 101: Securing Your Digital Environment

Episode 1: Laying the foundation

Question about a term?
Visit our Glossary

Welcome to MCNC's VitalCyber blog series, "Cybersecurity 101: Securing Your Digital Environment." Whether you're an administrator, IT manager, or cybersecurity professional, this series is designed to guide you through the essential steps of developing a foundational cybersecurity program.

We aim to demystify the process and provide practical, actionable insights and tools that you can use to build a strong foundation for your information security efforts. By the end of this series, we hope to give you a clear roadmap to protect your organization against cyber threats and secure your valuable data's confidentiality, integrity, and availability.

So, join us on this journey to fortify your organization's defenses and stay one step ahead in the ever-evolving information security landscape.

What's A Cybersecurity Program?

The first question you may have is, **"What exactly is a cybersecurity program?"** A cybersecurity program is the collective effort your organization puts into protecting your information assets from cyber threats. It consists of policies, processes, procedures, and technologies aimed at maintaining the confidentiality, integrity, and availability of your information assets. This program goes beyond just installing antivirus software or setting up firewalls; it takes a comprehensive approach to managing and minimizing risks related to information security.

Where To Start?

The next question may be, **"Where do I begin?"** Similar to starting construction on a house or a remodeling project, we recommend selecting a blueprint, obtaining the necessary permits, and taking stock of existing tools when building or remodeling a cybersecurity program.

- **Pick a Framework.** Selecting a security framework (our blueprint) is critical in building an effective cybersecurity program. A framework, such as CIS, NIST, or ISO, can provide a structured approach to risk management and mitigation, protection of information assets, process management, and enterprise development. Adopting a security framework simplifies your efforts to prioritize security initiatives, allocate resources efficiently, and measure progress over time, ultimately leading to a more resilient and secure organization. We will use the Implementation Group (IG) 1 and 2 safeguards from the Center for Internet Security (CIS) version 8.1 framework for this series to build our cybersecurity program.
- **The Information Security Policy.** One of the most critical steps, if not the most, in effectively implementing a cybersecurity program is securing the support and authority from senior leadership. This is typically outlined in an organization's information security policy (our permit). You should thoroughly review this policy and ensure that the cybersecurity program has been established and you, or more likely your job title, have the authority to execute it as per the policy and with the approval of senior leadership. This provides a firm foundation for

success. If your organization does not have such a policy, we have a template with the essentials you can use as a starting point.

- **Catalog existing controls.** When it comes to information security, we rarely begin with a blank slate. More often than not, we're building the plane while flying it. Start by documenting any administrative controls, such as policies, procedures, and guidelines concerning information security — likewise, catalog all technical controls that have been implemented, such as firewalls, intrusion detection systems, and encryption tools. This program overview helps you identify gaps, redundancies, and areas that need improvement. If you're unsure what to look for, here is a cybersecurity program framework you can use to get started.

Where Do We Go From Here?

Now that we have the essential building blocks—a framework, an information security policy, and an inventory of our existing controls—we're ready to build. Over the coming months, the blog series will cover the following 14 domains.

- Asset Management
- Software Asset Management
- Data Management
- Secure Configuration
- Account and Credential Management
- Network Management
- Application Security Management
- Vulnerability Management
- Audit Log Management
- Malware Defense
- Data Recovery
- Security Awareness Training
- Service Provider Management
- Incident Response Management

Each blog entry will highlight IG1 safeguards, also known as basic cyber hygiene, and additional topics related to more advanced safeguards included in IG2 to fill in the gaps and create a comprehensive cybersecurity program.

Take the Next Step in Strengthening Your Cybersecurity

Is your organization ready to enhance its cybersecurity posture? Our team of experts at MCNC is here to help. Whether you need a comprehensive risk assessment, policy analysis, or guidance on implementing best practices, we're ready to partner with you to safeguard your digital assets.

Don't wait until it's too late. Contact us today to schedule a consultation and discover how MCNC's Vital Cyber solutions can protect your institution. Fill out our Contact Us form and let's start building a stronger defense together.