Centrilogic

White Paper

5 MOST IMPORTANT PILLARS OF CYBERSECURITY YOUR ORGANIZATION SHOULD KNOW

October is “Cybersecurity Awareness Month,” an international campaign designed to help companies and the public learn about the importance of cybersecurity and take steps to protect themselves and their companies from cyberattacks. We asked our VP, Cybersecurity Practice, Steven Cohen to identify the 5 most important pillars of Cybersecurity every business should know.

1. KNOW YOUR SECURITY POSTURE

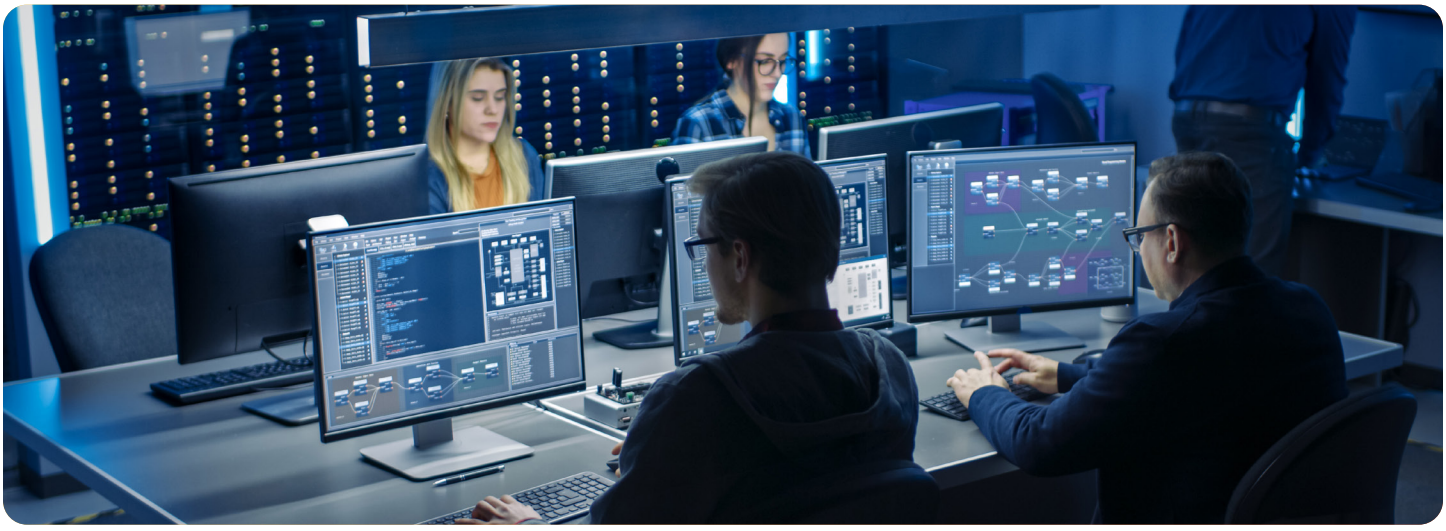
Do you know your security posture? Security Posture is defined by **NIST** as, "the security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes."

In other words, how you define, manage, evaluate, and react to cybersecurity issues dictates your security posture. Knowing your response capabilities is as important as performing regular assessments to identify cybersecurity gaps. These repeat evaluations allow internal teams to improve response and mitigation strategies, further optimizing your security posture. If you are unsure of your organization's security posture – or are concerned your organization is missing key components of an adequate security posture – we recommend that you invest in a comprehensive security assessment. To make the most out of your security assessments, pay attention to the **5 key steps every successful security assessment requires.**

THE TOP QUESTIONS TO ASK YOURSELF:

- Do we understand our organization's security posture?
- Do our employees have a security mindset?
- Do we have a process in place to respond to a security incident? If not, how vulnerable are we right now?
- Do we have a Cybersecurity Maturity Model?
- How do we measure up to a Cybersecurity Maturity Model?

Knowing where your organization stands in terms of cybersecurity also enables you to set expectations for how security breaches may be addressed or defended against, and gives you the means to educate others throughout the organization.

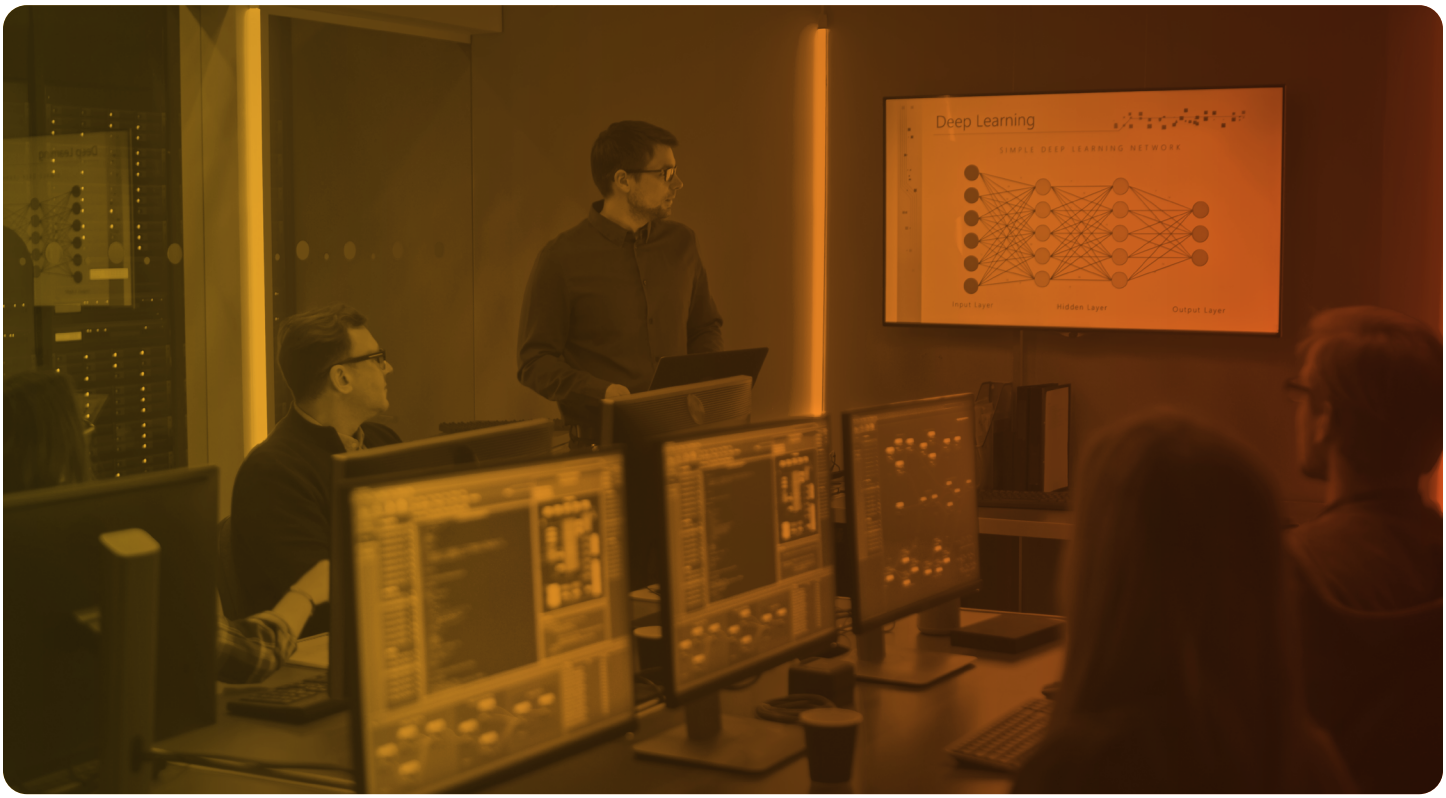


2. EDUCATE EVERYONE

It's a common misconception that only the IT team can stop cybersecurity threats. Your employees are your first line of defense.

Investing in cybersecurity education across your entire organization can improve your overall cybersecurity posture. Documenting and sharing vital information or cybersecurity best practices offers guidance to employees that will empower them to better identify any potential threats or incursions. This education will also enable them to make more effective use of mitigation measures should a threat or breach occur.

Within your organization, your security posture should be common knowledge. Employees should be able to understand the processes in place, and the technology that's being used to carry out those processes. Being educated on the fundamentals is key to preparing for security breaches and incidents that might impact your organization, business, or your employee's ability to do their job. Ideally, this practice is championed by an internal security leader. Many mid-market organizations, however, do not have a dedicated security resource. In that case, 3rd-party providers can deliver a **CISO-as-a-Service**, connecting you with experts who add leadership, value, and overall management of your cybersecurity portfolio.



3. BE PREPARED

Be prepared is a solid motto that should be applied to a lot in life, but especially when it comes to security.

The goal is to be proactive rather than reactive, allowing you to mitigate and defend against security breaches–before they can affect your business. This is why you want to **have a plan in place in the event of a security incident or breach**. Having that plan will offer much-needed guidance in a moment of crisis, empowering personnel to better manage the situation and its outcome. When you prepare enough, you learn how to adapt to new situations and protect your organization's digital assets in the face of **threats like ransomware**.

Knowing your security posture is the first step of being prepared for cybersecurity incidents. Preparation not only provides a sense of safety for your organization, customers, and clients, but it provides the means to really focus on the most mission-critical aspects of your cybersecurity.

4. FOCUS ON PRIORITIES

Too often, companies try to tackle everything at the same time. It's best to focus on only a few key areas and work to improve those first.

To make it easier to focus on your priorities, you might consider following an approach, like PPT (People, Process, Technology). People, Process, Technology is a methodology that helps organizations prioritize the most essential elements–the people, the processes the people follow, and the technology they leverage throughout the processes. Using a PPT approach, you'll begin to see how each of those elements interact with each other, which will help you prioritize not only the right people, processes, and technology, but also help document everything you need to educate your employees effectively.

The **NIST Cybersecurity Framework** is a more robust approach and a widely accepted Cybersecurity framework that IT teams can use to prioritize the different stages of handling security issues, such as Identifying, Protecting, Detecting, Responding, and Recovering. This type of framework emphasizes the importance of balancing proactive safeguards in the event of worst-case scenarios, which is especially important for small businesses where a worst-case incident could seriously impact the solvency of a business.

By focusing on select states or elements (such as in the PPT or NIST Frameworks), organizations gain the power to identify key gaps in compliance, learn who their largest targets are, and what the highest risk items are. Overall, they're able to leverage an adaptable methodology to manage their cybersecurity risk. While frameworks are guidance, organizations can still benefit from bringing in the right IT experts to field questions, fill in the gaps, or help with framework implementation.

5. BRING IN AN EXPERT

Every year, once thought leadership has been shared and advice is given on the latest cybersecurity threats throughout the month of October ("Cybersecurity Awareness Month"), digital attacks still rise up in the headlines. Organizations lose their footing because **cybersecurity is put 'out of sight, out of mind'** during the other eleven months of the year.

Not only is so much data and advice largely ignored throughout the year, but IT teams–from their composition to their function–also continue to evolve at a rapid pace, despite the lack of awareness in some organizations. When you look at how IT teams have changed over time, you begin to understand the importance of emerging specialties and the need for taking your cybersecurity more seriously.

As mentioned earlier, adopting a framework is excellent guidance for small businesses to undertake and can help them educate others in the organization and prepare for a disaster before it strikes. Unsure about the right processes or technologies? Not clear on what you're missing? Partner with Centrilogic – a team of cybersecurity professionals–to help you define what you are missing and build out a plan to improve your level of security today.