WHITE PAPER

THE CORNERSTONES OF A ROBUST SECURITY PROGRAM

Cyber security gets constant press. Unfortunately, amidst all the news about hackers, vulnerabilities, and data breaches, it is difficult to determine what you need to do to protect your organization and where to start.

When combined, the following security elements form the bedrock of a robust cyber security program

1 RISK TOLERANCE

Establishing your organization's risk tolerance is the best place to start when creating, or updating, your security program.

An organization's risk tolerance determines the necessary levels of data integrity, security and chain of custody services required to keep employee, company, and customer data safe.

Your organization's tolerance for risk is determined by your industry's regulations, compliance requirements, customer requirements and how much access to sensitive data your employees require to do their jobs.

2 SECURITY APPETITE STATEMENT

The next step is to create a security appetite statement. This document makes the security considerations established by your corporate risk tolerance official.

Ultimately, your organization's security appetite statement is a concise document that defines the level of risk senior management & the board of directors agree to. It formally establishes a balance between the security measures and business processes required to effectively manage risk while running the business.

3 ASSET AND CHAIN OF CUSTODY MANAGEMENT

The goal of asset management is to accurately inventory your organization's fleet of physical devices and software applications.

When an asset management program is coupled with a systematic approach to tracking an individual device's chain of custody, you will have the ability to track corporate owned devices and applications--giving your organization visibility to the corporate and non-corporate devices and applications that interact with your IT environment.

Strict chain of custody management also closes security gaps in the asset disposition process. Chain of custody validates the processes used to handle devices and destroy data are done in a way that mitigates risk and satisfies your security appetite statement.

4 ACCESS MANAGEMENT

Not everyone needs access to everything. Having the ability to manage a user's or an application's access to your corporate data is essential to a robust security program.

Access management is enabled by two things, tools and process.

You need tools that help your organization see what's going on within your IT environment so you can act quickly when anomalies are discovered. These include application based firewalls, network monitoring software, and centralized identity and access management software.

The key business process that aids access management is user segmentation. You will define how users are segmented as you establish your organization's risk tolerance.

Your employees should be segmented based on the data access requirements of their job. Additional segments should group employees by the location where they do their work–in the office versus in the field–along with other security considerations.

Each of your user segments will require different levels of access to data. Your organization needs to have the tools to enforce the access management framework outlined in your risk appetite statement.

5 INCIDENT RESPONSE PLAN

Your Incident Response Plan will function as a playbook for a range possible security incident types. It establishes the ground rules your organization will follow during security incidents.

A well thought out plan identifies who key responders are, their responsibilities, and how and when they are supposed to communicate with one another. It will also define things like when your organization is required to report an incident and other things easily forgotten when responding to a security event.

6 ONGOING SECURITY TESTING

Once your organization's security program has been implemented it must be tested. A combination of the following tests should be conducted regularly:

Tabletop Exercises: should be conducted to test and practice the incident response plan for a given security incident and should be performed annually at a minimum. The leader of these exercises will present 4 to 6 different incident scenarios and the incident response group will work through them to determine the organization's response. The composition of this group is important and should include key stakeholders within your organization. If possible your CIO, CISO, VP HR, CRO, Legal, and CEO should participate in the exercises.

PEN Testing: Conducting a penetration test on any new public facing element of your IT environment–like a new application or server–will help identify new security vulnerabilities. Once a new vulnerability is identified it can be dealt with accordingly.

Red Team Exercises: These exercises test both your security infrastructure and your response program through ongoing supervised ethical hacking initiatives.

7 SECURITY METRICS

Establishing and tracking security metrics is essential to measuring the effectiveness of your security program.

Most organizations will have different sets of security metrics; however, all robust security programs will categorize metrics in at least two ways, KPIs or Key Performance Indicators and KRIs or Key Risk Indicators.

Your organization's security metrics will be tied to the unique goals and requirements of your business, industry, risk tolerance, customer requirements, employee footprint, and more.

MCPc understands the security program that best protects your organization is developed with your unique security challenges and requirements in mind. MCPc's information security experts can help design, implement, and manage security programs that protect your data, your employees, your customers, and make your organization resilient in the event of a breach. We help clients adopt a culture of security that improves their success in managing and mitigating cyber risk.

CONTACT MCPc with your security questions:
www.mcpc.com/contact-us