Cybersecurity Basics

SecurIT360
The physics of securing IT

How can I build an effective information security program for my business?

This is a question that keeps many business leaders awake at night. For large companies and organizations, compliance requirements will often drive the need to meet at least the minimum standards of a good cybersecurity program. For small and medium businesses, the path is not always as clear. Good security is good security, whether your business is large or small. However, in many cases, smaller organizations may not have the staff, resources, budget or experience to build and maintain a good cybersecurity program.

A cybersecurity program can be complex, but it starts with a systematic, layered approach to the basics.

Identify Risks

An important first step is to identify security risks and the potential impact to your business. What areas of our security practice need improvement and what is the risk to our business if we do not fix them? It is important to identify the risks and express them in terms that are meaningful to your business.

Policy

It is critical to have documented policies regarding your IT systems, assets, processes, etc. NIST 800 standards are a good foundation for many organizations, but your policies must also include any compliance requirements of your industry. This must include a plan for continuous education of employees in respect to their personal, departmental and corporate processes and responsibilities. Policies should also include a third party technical testing and auditing schedule. If you do not have documented policies, an outside firm can be used to develop them for you.

Asset Management

You must know what you have, to manage it effectively. Every piece of hardware, software, data sets, and those that have access to them, must be identified and inventoried. Asset management also includes the documented processes for managing newly acquired assets.

Human Resources

Every organization should have a named HR director, even if that person has more than one responsibility or title. The HR Director should be involved in the process and documentation of training employees on internal security awareness. The hiring process should be documented and include security awareness training in the on-boarding of new employees.

Physical Security

Physical security is often thought of as separate issue, but it is a key component of information security. Access to areas where sensitive data or equipment is held, must be controlled and limited to those who need access to those areas. Policies for allowing non-employees into these areas must be documented and followed carefully.

IT Operations

One of the greatest potential operational risks can be the lack of experienced IT personnel and lack of controls to prevent data leakage. It is critical to have IT resources, whether internal or third-party, who have the experience, ability, and integrity to manage your IT environment and protect the sensitive information in your organization. Again, documented policies are required. If you use third-party resources, a clear definition of responsibilities, services, and scope of work must be included in the agreements drafted with these parties.

dburns@securit360.com

Cybersecurity Basics

SecurIT360
The physics of securing IT

Access Control

Personnel should only have access to the systems and equipment needed to be effective in their role within the organization. Every user should have a unique user id and password for any system they use. Passwords should never be shared and default passwords should never be used. Password policies should require complex passwords which are changed on a regular schedule. Controls must be in place to prevent unauthorized access to the network.

Systems Lifecycle

Documented policies and procedures for system lifecycles are required. This includes media disposal processes and processes for patching workstations.

Backup/Recovery

Every organization should have the ability to backup and recover their data. Backup tapes and drives should be encrypted and kept offsite. Documented procedures for disaster recovery and business continuity are critical.

Privacy/Compliance

There should be a function within the organization to stay apprised of current regulations or requirements and provide internal accountability for security and compliance. Third party technical testing and auditing should be done at regular intervals to prove the effectiveness of your information security program.

As stated above, good security is good security for any organization. However, it is important to take a thoughtful approach to all of these areas to be sure that your information security program is appropriate and effective for your organization.

As always, develop a “cyber-defense” mindset to protect yourself AND your company.

If you would like to learn more about Cybersecurity and how to protect your company, contact -

David Burns
Account Manager, SecurIT360
dburns@securit360.com
205.787.1250