How to Develop a Cyber Security Program

An Online Continuing Education Course for Engineers

Course Number: FM-4004

Credit: 4 Hours / 4 PDH / 4 CPD

How to Develop a Cyber Security Program

Lee Layton, P.E.

Introduction

Businesses – both large and small - need to protect against growing cyber threats. As larger companies take steps to secure their systems, less secure small businesses become easier targets for cyber criminals.

This course is designed to assist small engineering firms and other small businesses secure their operations by using practical and sensible guidelines. The course is designed for businesses that lack the resources to hire dedicated staff to protect their business, information and customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this information.

The guidance in this course was developed by the FCC with input from public and private sector partners, including the Department of Homeland Security, the National Cybersecurity Alliance and The Chamber of Commerce. In 2009 the Department of Homeland Security created an ongoing cybersecurity awareness campaign called "Stop.Think.Connect.™". The FCC also has a small business planner tool that allows a business to develop a customized cyber security policy for the specific business.

This course discusses scams, network security, websites, email, mobile devices, employees, facilities, credit & debit cards, and policy development for cyber security protection.

Chapter 1: Scams and Fraud

New telecommunication technologies offer countless opportunities for small businesses, unfortunately they also offer cyber criminals many new ways to victimize a business, scam customers and hurt the company's reputation. Businesses of all sizes should be aware of the most common scams perpetrated online.

> 44% of small businesses have reported being a victim of a cyber attack with an average cost of $9,000 per attack.
>
> Source: National Small Business Assn. 2013

Cyber Plan Action Items:

1. Train employees to recognize social engineering

Social engineering, also known as *pretexting*, is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information and/or installing malicious software onto their computers, devices or networks. Social engineering is successful because the bad guys are doing their best to make their work look and sound legitimate, sometimes even helpful, which makes it easier to deceive users.

Most offline social engineering occurs over the telephone, but it frequently occurs online, as well. Information gathered from social networks or posted on websites can be enough to create a convincing ruse to trick employees. For example, LinkedIn profiles, Facebook posts and Twitter messages can allow a criminal to assemble detailed dossiers on employees. Teaching people the risks involved in sharing personal or business details on the Internet can help a company partner with its staff to prevent both personal and organizational losses.

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software such as fake antivirus, thinking they are doing something that will help make them more secure. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker, unwittingly installing software that can steal financial information or simply try to sell them fake security software.

2. Protect against online fraud

Online fraud takes on many guises that can impact everyone, including small businesses and their employees. It is helpful to maintain consistent and predictable online messaging when communicating with customers to prevent others from impersonating the company.

Be sure to never request personal information or account details through email, social networking or other online messages. Customers should be notified that the company will never request this kind of information through such channels and instruct them to contact the company directly should they have any concerns.

3. Protect against phishing

Phishing is the technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. Small businesses face this threat from two directions -- phishers may be impersonating them to take advantage of unsuspecting customers, and phishers may be trying to steal their employees' online credentials.

Businesses should ensure that their online communications never ask their customers to submit sensitive information via email. Companies should make a clear statement in communications reinforcing that it will never ask for personal information via email so that if someone targets customers, they may realize the request is a scam.

Employee awareness is the best defense against users being tricked into handing over their usernames and passwords to cyber criminals. Explain to everyone that they should never respond to incoming messages requesting private information. Also, to avoid being led to a fake site, they should know to never click on a link sent by email from an untrustworthy source. Employees needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

This advice is especially critical for protecting online banking accounts belonging to the organization. Criminals are targeting small business banking accounts more than any other sector.

4. Don't fall for fake antivirus offers

Fake antivirus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds in recent times. Make sure the organization has a policy in place explaining what the procedure is if an employee's computer becomes infected by a virus.

Train employees to recognize a legitimate warning message and to properly notify the IT team if something bad or questionable has happened. If possible, configure computers to not allow regular users to have administrative access. This will minimize the risk of them installing malicious software and condition users that adding unauthorized software to work computers is against policy.

5. Protect against malware

Businesses can experience a compromise through the introduction of malicious software, or malware, that tracks a user's keyboard strokes, also known as *key logging*.

Many businesses are falling victim to key-logging malware being installed on computer systems in their environment. Once installed, the malware can record keystrokes made on a computer, allowing bad guys to see passwords, credit card numbers and other confidential data. Keeping security software up to date and patching computers regularly will make it more difficult for this type of malware to infiltrate the network.

6. Develop a layered approach to guard against malicious software

Despite progress in creating more awareness of security threats on the Internet, malware authors are not giving up. Effective protection against viruses, Trojans and other malicious software requires a layered approach to defenses. Antivirus software is a must, but should not be a company's only line of defense. Instead, a combination of techniques is needed to keep the environment safe.

Also, be careful with the use of thumb drives and other removable media. These media could have malicious software pre-installed that can infect a computer, so make sure the source of the removable media devices is trustworthy before using them.

Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with operating system and applications increases the safety of systems.

7. Verify the identity of telephone information seekers

Most offline social engineering occurs over the telephone. Information gathered through social networks and information posted on websites can be enough to create a convincing ruse to trick employees.

Ensure that employees are trained to never disclose customer information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and their request.

Chapter 2: Network Security

Securing the company's network consists of:

1. Identifying all devices and connections on the network;
2. Setting boundaries between the company's systems and others; and
3. Enforcing controls to ensure that unauthorized access, misuse, or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Cyber Plan Action Items:

1. Secure internal network and cloud services

The company's ne et by strong user authentication me s firewalls and web filtering proxies. Additiona irus software and intrusion detection systems, icious code or unauthorized acces

Internal network

After identifying the boundary should be evaluated to determi nd how they can be best deployed. Border rou nd from the company's public IP addresses, fi and from the minimum set of neces uld be configured to monitor for suspicious prevent bottlenecks, all security systems de perimeter should be capable of handling the bandwidt provides.

Cloud based services