Cyber Security Action List

Prioritise cyber security within the organisation: This should be pushed from top down. Cyber security should be discussed with the Board of Directors and senior management. Identify information security and incident response team, including legal, compliance and business leads for cyber security matters.

Review existing policies: Review existing information security policies and procedures ensuring they reflect current regulatory requirements and that all applicable regulatory requirements have been built into company procedures.

Account for every device: Know where your firm data resides including not only servers and workstations, but mobile devices, thumb drives, backup systems and cloud locations. Audit every device with access to your network. With the rise in BYOD this has never been more important.

Implement enterprise-grade security software: Cover your network, email and endpoints with regularly updated antivirus, antimalware and real-time detect and respond capability

Keep on top of updates: Keep every device updated regularly, ensuring there are no weak areas

Use automatic screen lock: Automatically lock screens on all devices to keep prying eyes away from the system.

Dispose of data/equipment properly: Legacy files and documents with personally information should be secured and shredded. Workstations and other mobile equipment used for processing client data should be thoroughly reformatted or the hard drive physically destroyed to minimize the risk of nefarious data recovery.

Encrypt backup data: Firms should encrypt any backup media that leaves the office and also validate that the backup is complete and usable.

Continuously monitor traffic: Traffic analysis can be the key to revealing intruders. A rise in activity could Indicate a Trojan within the network.

Enable remote wipe on employee devices: Erasing data in the event of loss or theft can minimise damage.

Implement multi-factor authentication: The more layers of protection, the harder it is for a hacker.

Educate staff: Most cyber-attacks are caused by employee negligence or malice. Ensure every employee is aware of cyber security and prevent basic mistakes.

Conduct periodic risk assessments: Risk management principles apply to information security. Conduct periodic risk assessments to identify cyber security threats, vulnerabilities and business consequences.

Carry out checks on vendors: Verify that third-party vendors have sufficient cyber security insurance coverage.

Obtain cyber insurance: Ensure your cyber insurance cover is adequate.

Millennium Affine provides a range of cyber security services including: risk assessment, penetration testing and vulnerability assessment, development of a written information security policy (WISP), development of an incident response plan (IRP), identification of critical third parties and provision of a comprehensive risk management review (RMR), sensitive and critical data identification, phishing tests and on-going cyber security advisory services.

To discuss how we can help you keep your organisation secure call us on +44 (0) 845 604 4262, email info@millenniumaffine.com or visit millenniumaffine.com.

Millennium Affine

Cyber Security Threats

Trojan: Hides itself from antivirus detection, steals important data and can even take over entire security systems.

Virus: A malicious program which replicates itself, corrupting the computer system and destroying data.

Worms: Does not alter a system but can spread from one computer to another within a network.

Spyware: Is Malware designed to spy on the victim's computer.

Scareware: Planted in a system which informs the user that they have an infection which doesn't exist. The idea is to trick the user into purchasing a bogus anti-malware.

Keylogger: Records every key-stroke made on a keyboard. It's a powerful threat used to steal people's login credentials such as username and password.

Adware: This is when pop up adverts occur. It is not harmful but can be annoying.

Backdoor: A method where attackers can bypass all the regular authentication service. It is usually installed before any virus or Trojan infection to ease the transfer effort of those threats.

Wabbits: A self-replicating threat which doesn't harm the system like a Virus or replicate like Worms.

Cookies: Not Malware but used by most websites to store information on computers. Has the ability to store and track your activities within the site.

Exploit: A form of software which is programmed specifically to attack certain vulnerabilities.

Botnet: Installed by a BotMaster to take control of all the computer bots via the Botnet infection, which can then be used for a large scale attack.

Dialer: Uses an internet modem to call costly international numbers. This was popular in the past with dialup modems but today, is more popular on Android because it can use phones to send SMS to premium numbers.

Dropper: Designed to drop into a computer and install something useful to the attacker such as Malware or Backdoor. There are two types of Dropper; one immediately drops and installs to avoid Antivirus detection, the other will only drop a small file to auto trigger a download process to download Malware.

Fake AV: Users seldom face a virus infection but are scared into purchasing a bogus antivirus which does nothing.

Phishing: A fake website which is designed to look like the actual website. Tricks the user into entering personal details into the fake login form which allows the identity of the victim to be stolen.

Bluesnarfing: Unauthorised access to a specific mobile phone, laptop, or PDA via Bluetooth. By having such unauthorised access, personal items such as photos, calendar, contacts and SMS can be revealed.

Boot Sector Virus: A virus that places its own code into the computer DOS boot section.

Bluejacking: Uses Bluetooth technology but isn't as serious as Bluesnarfing. It connects to a Bluetooth device and sends messages to other Bluetooth devices.

DDoS: Sends a high volume of traffic to a single server. This can cause systems to go down with certain security features disabled so data can be stolen.

Browser Hijackers: Uses the Trojan Malware to take control of the victim's web browsing session.

Virus Document: Spread via document files and PDF documents.

Mousetrapping: Traps your web browser to a particular website. Automatically redirects users back to the site if they try and navigate off.

Obfuscated Spam: Spam mail which doesn't look like a spamming message and tricks victims into opening it.

Pharming: Similar to phishing. There are two types of pharming; DNS poisoning (where the users DNS is compromised and all traffic is redirected to the attacker's DNS) and another where the HOST file is edited, redirecting users to another site.

Crimeware: A form of Malware which takes control of the users computer to commit a computer crime. Instead of the hacker committing the crime, they plant a Trojan to order the user to commit a crime instead.

SQL Injection: SQL injection does not infect the end users directly; it infects a website which is vulnerable to attack. It then gains unauthorised access to the database in order to steal data.

This is a selection of the cyber security threats commonly found today. New ones are being regularly developed and the battle to combat them remains on going.