IT Security Brief Checklist

Right Networks®

Introduction

As technology and security threats continuously evolve and affect a firm's computer and internet use, owners must ensure that all firm personnel are aware of resulting changes in firm policies and IT practices.

The best way to do this is to mandate that all personnel participate in an IT security briefing at least once a year. The IT security briefing should inform personnel of the firm's updated policies, security threats, best practices for minimizing IT risks, and how to respond when a questionable event occurs.

Conducting the IT security briefing annually makes it possible to communicate needed updates and remind firm personnel of all policies. The following checklist includes key areas to cover during your next annual IT security briefing.

Policy Review and Updates

- ☐ Review the firm's IT policies for computer and internet use, remote accessibility, smart phone and tablet use, digital client confidentiality, social networking, and sharing passwords with firm members.
- ☐ Review specific changes and show personnel how to access the firm's IT policies.
- ☐ Quiz firm members on policy changes to ensure they are aware of them.

Passwords and PINs

- ☐ Passwords should be changed at least quarterly, using complex passwords and passphrases. Passwords should be at least eight characters and include an upper- and lower-case letter, along with a number and special character.
- ☐ Firm members must be trained to NEVER share passwords or PINs with anyone.
- ☐ Firm members should be educated on "social engineering" attacks designed to elicit disclosure of information that can be used to expose the firm's security and client data.
- ☐ Firm members should be trained on what to do in the event that a password is disclosed.

Workstation Protection

- ☐ Workstations should be set up for automatic updates of operating systems, browsers and key security applications, such as anti-virus and spyware tools, so that they can't be circumvented or uninstalled.
- ☐ Firm members should be reminded of the importance of workstation protection and told specifically NOT to turn off their firewall or download any non-firm applications to a local workstation without the IT team's knowledge and approval.
- ☐ Alert firm members that one of the most common attack methods is a message that pops up when browsing a website that states that the computer's system has been breached and that the user should immediately download a fix or call a phone number on the screen for help.

- ☐ Firm members should be aware of how to safely close a suspicious pop up message (Ctrl+F4) without downloading any malware. If the workstation begins to perform erratically or slowly, the user should notify IT support immediately.

Email Threats

- ☐ Remind firm members how to identify and deal with suspicious emails.
- ☐ Alert firm members to current phishing, spear-phishing, and pharming threats.
- ☐ Remind firm members that threats can take many forms, including: email, instant messaging, or pop-ups on any of their screens.
- ☐ Offer information on how to spot a suspect email address, email subject or attachment name and how to verify the actual sender/hyperlink.
- ☐ Encourage users to take the OpenDNS phishing quiz to practice discerning between real and fake websites.
- ☐ Remind firm members to be on the lookout for generic (“Dear User”) or incorrect salutations instead of their name, obvious grammatical or spelling errors within the body of the text, alarmist messages (“Your information has been breached; click here to minimize your loss.”) or ANY request for personal logins or passwords.
- ☐ Remind firm members to NEVER use a hyperlink from within an email that would link to any confidential resources. Instead, they should open a new window and type in the site they want to visit.
- ☐ Firm members should also be made aware that telephone numbers listed within suspicious emails can also be linked to fake call centers, so care should be taken to verify that the number is valid before calling. For more information on current email scams, turn to the Snopes.com website, which is frequently updated and easy to search.

Confidentiality

- ☐ Firm members should not transmit client, firm or any personal information via email or instant messaging unless there are encryption tools or verified secure (SSL) connections in place, especially when using public or client internet access.
- ☐ Firm members should be required to use the firm’s selected method, such as secure portal and/or encrypted email service and be directed to ask clients do the same.
- ☐ Confidentiality should also extend to work in remote sites. Firm members should be educated to protect their screen with a privacy filter if there is a potential that someone could view their client data.
- ☐ Firm members should be taught that all public WiFi sites are unsecure as it is easy for thieves to create “Free WiFi” sites or to log activity on these sites.

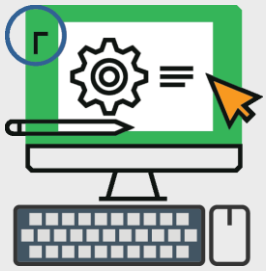
Physical Security

- ☐ Remind firm members about physically securing devices, since a stolen laptop, lost smartphone, misplaced USB thumb drive or an unsecured door can lead to a security breach.
- ☐ Internet-enabled devices should always have a secure PIN/password and any client data residing on them should be encrypted.

- ☐ Remind firm members to use privacy filters when working in public places.
- ☐ Remind firm members that all digital data on hard drives and thumb drives should be encrypted.
- ☐ Remind firm members to digitally lock their computer screen(s) when not in use and always have their devices in their possession or physically locked to a desk if they leave their work area.
- ☐ Educate firm members on IT breaches that have happened to other firms and the firm's related policies.

The greatest vulnerability for most firms is personnel ignorance of computer and security policies and/or failure to adhere to them.

An annual reminder and update of the policies will go a long way towards minimizing the risk of falling victim to a security breach.



Learn more at
www.rightnetworks.com