Institute of Engineering & Management

Recruiting for cyber security: What businesses need to know

When it comes to cyber security, figuring out what you need is the easy part. Figuring out who you need, can be tricky. Cyber security has gone from being a diversion for amateur hackers to a legitimate business threat. Attacks on infrastructure now represent a major concern for organisations of all sizes, meaning cyber security professionals are currently in incredibly high demand – and accordingly in limited supply. There have been multiple very well-documented cyber-attacks in recent years.

FACT

Last year, cyber-crime cost companies across the world $445bn in revenue, and 150,000 employees are expected to lose their jobs due to downsizing related to these attacks. The reality is that there is nothing more business-critical than a solid cyber security strategy, because without one you may well end up unable to do business in the first place.

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

Creative Search

The positions you need to fill may not even exist or might be in limited supply, especially where your organisation is most innovative. Taking a macroscopic view in understanding the key drivers and the objectives – as well as finding complementary technology solutions or processes – will be the key to unlocking your challenges. This will ultimately broaden your search area and enhance your possibilities.

Partnering with educational institutions seems to be an emerging theme. As research-led entities, universities can potentially have access to the best and most up-to-date information in the cyber security field. Collaborating with their academics on developing these courses can be a good way to access the information you need to formulate your recruitment strategy.

Whatever you do, a robust security strategy should be a top priority for your business. Where possible, it should be integrated from the very start. Retrofitting it to an unsuitable IT infrastructure is a much harder task, and even more so in this hyper-competitive market.

It is easy to think that because cyber security is a “hot button topic” that it’s also overblown – like an IT version of swine flu. It is also easy, even if you do acknowledge its importance, to allocate resources to other more seemingly business-critical departments.

What is fake antivirus?

Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. The malware makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program. It also causes realistic, interactive security warnings to be displayed to the computer user.

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

USING WIFI: CONNECT WITH CARE

Wi-Fi in airports, hotels, train stations, coffee shops, and other public places can be convenient, but often these hotspots are not secure, and can leave you at risk. There are precautions you should take to make sure your personal information is safe. First and foremost, connect with care. If you're online through an unsecured network, you should be aware that individuals with malicious intent may have established a Wi-Fi network to eavesdrop on your connection. This could allow them to steal your credentials, financial information, or other sensitive and personal information. It's also possible that they could infect your system with malware. Any free Wi-Fi should be considered "unsecure." Therefore, be cautious about the sites you visit and the information you release.

STOP. THINK. CONNECT.

Few tips to remember when using Wi-Fi:

Keep your computer and mobile devices updated. Having the latest version of security software, operating system, web browser and application can help protect you from malware and other threats you may encounter when using Wi-Fi. Don't assume that the Wi-Fi connection is secure. Many hotspots don't encrypt the information you send on the Wi-Fi network. Do not log into accounts, especially financial accounts, when using public wireless networks. Do not log onto sites that seem suspicious (clues include the URL being misspelled or not matching the name that you were given by the place of business). It's not uncommon for cybercriminals to set up a Wi-Fi network called "free Wi-Fi" in airports, hotels, and other public places. A cellular 3G/4G connection is generally safer than a Wi-Fi connection. Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi.

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091