Cyber Risks & Liabilities

July/August 2023

Attack Surface Management Explained

Attack surfaces refer to the total possible entry points (also known as attack vectors) for unauthorized access into any system. The recent rise of remote and hybrid work combined with the shift to the cloud and widespread implementation of software-as-a-service applications have made attack surfaces increasingly prominent, complex and difficult to defend against cyberattacks. Fortunately, attack surface management (ASM)—the continuous monitoring of potential attack vectors—can provide organizations with an inventory of exposed assets to accelerate responses to cyber threats. ASM entails the following automated core processes:

1. **Asset discovery**—This is a continuous process that scans for potential entry points for cyberattacks. These assets may include subsidiary assets, third-party or vendor assets, unknown or non-inventoried assets, known assets, or malicious or rogue assets.
2. **Classification and prioritization**—Assets are analyzed and prioritized by the likelihood that hackers could use them as a target. They're inventoried by their connections to other assets in the IT infrastructure, such as IP address, identity and ownership. Assets are also analyzed for exposures such as missing patches, coding errors and potential attacks, including ransomware or malware. Each vulnerable asset is assigned a risk score or security rating.
3. **Remediation**—Potential vulnerabilities are remediated in order of priority. It may be necessary to apply software or operating system patches, debug application codes or use stronger data encryption. Previously unknown assets may need new security standards, or it may be necessary to integrate subsidiary assets in organizations' cybersecurity strategies.
4. **Monitoring**—Security risks change whenever a new asset is deployed or existing assets are used in new ways. Networks and their inventoried assets are continuously monitored for vulnerabilities to allow ASM to find attack vectors in real-time and give organizations a chance to neutralize threats.

ASM not only protects organizations from cyberattacks, but it's also frequently required by underwriters to obtain cyber insurance, making it all the more vital.

Contact us today for additional risk management information and insurance solutions.

Case Insurance Brokers Inc.
336 Millwood Road
http://www.caseinsurance.ca

Case
INSURANCE BROKERS

Buying and Selling Secondhand Devices

Employees sometimes access work-related systems from their personal electronic devices. While this can help get tasks done sooner, it can also leave an organization vulnerable to stolen information or data breaches if that personal device is ever compromised, such as when it's resold. That's why it's crucial to ensure all data is thoroughly deleted prior to reselling a device. Share the following tips with employees to help avoid potential data compromises:

- Use the "factory reset" feature to erase all personal data from devices, including messages, contacts, photographs, browsing history, Wi-Fi codes passwords and any installed apps. For assistance, check the manufacturer's guidelines for the specific device.
- Select "no" if given the option to keep personal files when erasing data unless the device is being kept.
- Check that secondhand devices are supported by the manufacturer and still benefit from regular security updates when buying such devices. Additionally, perform a "factory reset" to ensure that devices are ready for first use.

By sharing these few simple steps, employers like you can help employees keep both personal and company data secure when buying and reselling electronic devices.

How to Use Public Wi-Fi Safely

Public Wi-Fi allows employees to access online accounts, catch up on work and check emails on the go. Unfortunately, while convenient, it isn't risk-free. Cybercriminals can attempt to hack into a device through unsecured Wi-Fi networks or eavesdrop on Wi-Fi signals to access personal information and login credentials. They may also use an unsecured Wi-Fi network to spread malware to other devices on the network. Moreover, some public Wi-Fi networks can even be fake hot spots that lure users with a similar name to the legitimate hot spot.

To avoid these types of situations, employees should follow these tips to use public Wi-Fi networks safely:

- **Turn Wi-Fi off when it's not being used.** Most devices that connect to Wi-Fi have a way to turn it off. When Wi-Fi isn't needed, toggle that feature off so the device won't search for it or connect to nearby networks.
- **Use a firewall**. When possible, install a firewall on devices. A firewall is a security barrier between two networks that control the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
- **Use a virtual private network (VPN).** When utilizing public Wi-Fi often, it's a good idea to use a VPN; it directs all web activity through a secure, independent network that encrypts and protects a user's data. Most internet service providers offer a VPN as a secondary service.
- **Browse securely.** Never trust wireless encryption on a public Wi-Fi network. Instead, ensure websites scramble data by enabling secure socket layer encryption in the settings of the sites being visited. Additionally, ensure websites use HTTPS, which is more secure than regular HTTP sites.

By its very nature, public Wi-Fi can expose your organization to additional cyber risk because you can't see or control who has access. However, by communicating with employees the importance of safe public Wi-Fi use, you can lessen the risk and bolster your cyber resilience in the process.

For additional cybersecurity tips, contact us today.