Cyber Security Best Practices

Ransomware Protection / Data and Email Encryption

Ransomware Protection

Ransomware is all the rage these days. The news is full of horror stories where hackers encrypted all the data on a company's server and they had to pay a ransom in cryptocurrency to get it back. Without the decryption code, your data is gone. Ransomware is two-pronged: **endpoint detection and response and consistent data backups.**

Endpoint Detection and Response

Ransomware is detectable, either at the point it is delivered to a PC, or when it deploys. Endpoint detection involves catching the ransomware at work. The response usually involves isolating the infected PC from the rest of the network before it can spread. EDR is an excellent add-on to your existing antivirus program.

Data Backups (& Passwords)

The ultimate defense against ransomware is a reliable point-in-time data backup. Ensure that the feature of automatic backups is scheduled to run multiple times per day so that you don't lose work by accident, or any other reason. Backups should be encrypted and password-protected.

Passwords should also be force-changed periodically; 30-90 day rotations are recommended. If possible, utilize a password manager that can automatically generate strong passwords for each website or application your company utilizes.

Data and Email Encryption

Data can be encrypted in two ways: **at rest and in transit.**

Encryption at Rest

This involves encrypting the hard drives where data is stored. This way, even if the laptop is stolen, the data residing on the laptop cannot be accessed. Activating an encryption protocol will create a recovery key which must be retained. Without it, your data will be unavailable.

Encryption in Transit

This refers to data while it is being moved or transferred, usually through electronic communication like email. If you send and receive protected information, you should consider a system that will encrypt the email so it cannot be compromised in transit.

The Uhl Agency

Cyber Security Best Practices

Gateway Security / Multi-Factor Authentication

Gateway Security

This refers to the outermost layer of your IT system - essentially the spot where your network touches the internet by way of router or modem. Most internet service providers have minimal or no firewall capabilities. You should invest in a robust firewall that includes virus scanning, intrusion and hacking prevention.

Antivirus Protection

Every PC or server on your network should have an antivirus program that does both on-access scanning and does a scheduled daily full scan of the hard drive. If a virus is found, the administrator of your network and the affected user should be notified by the antivirus program.

Email Filtering

The primary avenue for hackers to gain access to data or engage in their nefarious practices these days is via email. Third-party services are available to scan and remove emails that may be spam, phishing, or contain a virus. Most email systems have these features, but the add-on of paid services can add an increased level of security.

Multi-Factor Authentication

Multi-factor authentication (MFA) or two-factor authentication (2FA) are processes where, after your initial entry of user name and password onto a PC, laptop, tablet, or other device, a token is sent by way of a text message, email, voice message or an authenticator app on a mobile device. This token provides a secondary method of authentication to verify the identity of the user.

Email Two-Factor Authentication

This form of two-factor authentication is built specifically for your email. This is now built-in to most email providers and simply needs to be activated. You won't have to authenticate every time you check your email at your PC, and it is customizable for how often you're prompted to approve your request. If this isn't available through email, you should implement 2FA at a minimum for users to log onto company owned devices.

The Uhl Agency

Cyber Security Best Practices

Additional Security Steps

Written Policies

In the event of a breach, written policies can be very helpful. Putting these policies and procedures into your employee handbook help to communicate the rules and procedures regarding cybersecurity and establish proper security standards.

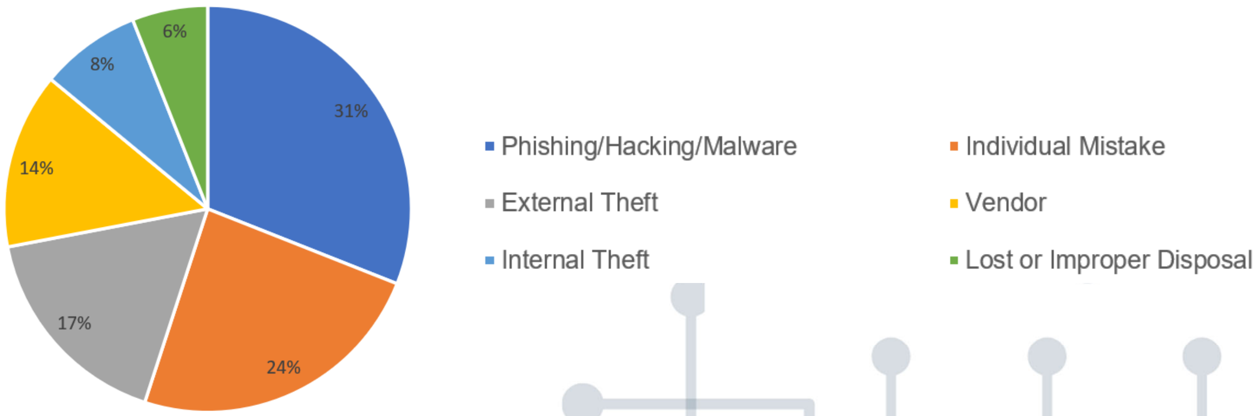
Remote Access

Many people are working remotely. Remote access should be secured by a VPN or an industry-standard remote control program with two-factor authentication enabled.

User Education

It is important to educate your users of fraudulent emails and messages. Today's hackers are very sophisticated and many of them craft messages that are extremely deceptive and believable. Teach employees to understand and recognize certain giveaways when it comes to suspicious emails.

Causes of Ransomware Attacks



Alerts & Notifications

It is important that your or your IT provider be notified if there is a breach. Also, staff should notify someone if they get a suspicious email or other unusual event.

Response Plan

The potential damages from a data breach extend to more than just a loss of your data or your customer's. There is a certain amount of reputational damage as well. Having a response plan in the event of a breach, including notifying affected parties can help mitigate the damage.

Cyber Insurance

While cyber insurance may not prevent a cyber attack from occurring, many cyber insurance policies provide tools that assist with evaluating and bolstering your network security. In addition, should a breach or attack occur, cyber insurance can assist with covering the expenses associated with the event, including customer notification costs, forensic costs, loss of income, reputational repair costs, and more. Contact The Uhl Agency at 937-434-9090 to learn more!