Cyber-Security Overview

Today's news has no shortage of stories profiling cyber-security incidents including theft, breaches, and data loss. Often, the incidents that we hear about are related to large businesses. Because of this, many small businesses have a false sense of security as they feel they are not of interest to attackers.

However, the facts state that small and mid-size businesses have a higher risk of being targets for cybercriminals. This is because small and medium businesses (SMB's) do not have the controls in place to prevent or deter threats in the modern IT landscape. Due to this, cybercriminals often see SMB's as 'soft targets' where their attacks can be more successful and profitable than if they target a large business that has a modern and mature security infrastructure in place.

According to a 2018 Data Breach Investigations Report by Verizon, 58% of call cyber-attacks targets small & medium businesses. This is for the simple fact that they are easier to penetrate. In other words, cyber-criminals are counting on small and medium businesses to have outdated network security measures and little to no protocols in the event of an attack.

Types of Cyber Attack

- **Malware** – this is software is intended to damage or disable computers and computer systems. This can be in the form of a virus, spyware, ransomware, adware, and more.
- **Ransomware** – this is a type of malware is designed to deny access to a businesses computer system(s) and data until a monetary ransom is paid. Often, the ransom is paid and the attacker never returns the data.
- **Trojan Horses** – this is a type of malware hidden within a seemingly legitimate application. This misleads the user about an application's true intent, which is to perform some type of damaging function to their network.
- **Phishing** – this is like fishing on the water. Instead of trying to catch fish, attackers are fishing for your personal information. An attacker will often send an email that portrays itself as a trusted source in an attempt to coerce the recipient to provide credit card, banking and other sensitive information.
- **Unpatched Software** – patching is necessary to keep your system~~s~~ current with the latest security fixes. Attackers are constantly learning how to exploit common applications such as Microsoft Windows, Adobe, etc. When a vulnerability is discovered in the application, the provider will release a patch which can be downloaded to seal any exploits.

How to Protect your Business

Vigilance

Stay up to date on the latest trends and advancements in cyber-security. Work with a partner who is an expert in this area and have them provide you with frequent recommendations. Have your IT team attend the latest conferences and review what other businesses are doing to protect themselves.

Empower your People

Educate your employees and have them understand how cyber-security effects the bottom line of your business. A good IT partner will provide annual lunch & learns to teach your staff about online threats and what they can do to protect themselves.

Limit Access to Information

Keep your data on a ‘Need to Know’ basis. Make sure your business~~es~~ data is accessible only to staff members authorized to access it. Your IT partner will be able to help setup walls between groups of data so only those who need to know will have access.

Patch promptly

A strong patch management practice is imperative to maintain good cyber-security hygiene management. This can be a complicated process considering factors such as the size of your network, the applications you are using, etc. It is recommended you patch all systems on a monthly basis using a combination of manual and automated processes.

Encrypt Data

In the event your encrypted data is stolen, it will be rendered useless to the attacker if they do not have access it. You can do this by creating a strong password policy using a combination of special characters and numbers. A good rule to follow is to frequently change your passwords.

Consult an Expert

Spend more time focusing on your core business by having an expert advise and manage cyber-security measures on your behalf. AlphaKOR has decades of experience in this area. Our Team can provide you with guidance on the how to keep your business~~es~~ safe from cybercriminals in the modern age.

Conclusion

A good cyber-security practice does not require a massive investment in technology. However, it is advised to keep your systems current, ensure you and your staff are aware of the dangers, and have a plan of action in the event a cyber-security incident occurs. In the modern threat landscape, knowledge is power and information is gold. Arm yourself with the knowledge required to safeguard your information, your staff, and your business. And if you have any questions on how to do this, always feel free to call AlphaKOR.