ROARK TECH SERVICES

15 WAYS TO PROTECT YOUR BUSINESS FROM A CYCBER ATTACK

1. SECURITY ASSESSMENT

It's important to establish a baseline and understanding of existing vulnerabilities. When was your last assessment? If the answer is "never", you are at greater risk than you think.

2. PHSYICAL SECURITY

This is an often-overlooked piece of a cybersecurity program. Keeping uninvited guests out of your office and securing sensitive areas is a crucial step toward protecting your data and your business from breaches.

3. FIREWALL

Your firewall monitors and controls incoming and outgoing network traffic based on security rules. This is the barrier between a business and an untrusted actor. Turn on Intrusion Detection and Intrusion Prevention features.

4. OPERATING SYSTEM & APPLICATION UPDATES

Keep your Operating System and suite of applications updated for better security. Ensure up-to-date versions of all your critical software. Windows 7 and Office 2013 are no longer supported and therefore Microsoft is not producing security patches for them.

5. MULTI-FACTOR AUTHENTICATION

Utilize MFA whenever and wherever you can, including on your network, remote access, banking / accounting / shopping websites, social media and any other devices your business uses.

6. PASSWORD COMPLEXITY

Apply security policies on your network that require complex password or passphrase creation with mandatory special characters, letters, numbers and at least one capital letter. Employ a password manager to help keep track of complex passwords.

7. SECURE OFF-SITE BACKUP

Backup locally. Backup to the cloud. Maintain an off-site backup that is not connected to the Internet. Backup often. Test your backups periodically and secure them with a complex password.

8. SECURITY AWARENESS

Train employees often. Teach them about data security, e-mail attacks and the reasons behind your cybersecurity policies and procedures. Employees are the weakest link in your security chain.

9. MOBILE DEVICE SECURITY

Today's cybersecurity criminals attempt to steal data or access networks through employee phones and tablets. They count on the businesses neglecting the security on these devices.

10. ENCRYPTION

Whenever possible, the goal is to encrypt data at rest, in motion and especially on any mobile device.

11. END POINT DETECTION

Protect data from malware, viruses and cyberattacks with advanced endpoint security. Today's technology protects against "file-less and script-based" threats and even roll-back a ransomware attack.

12. E-MAIL PHISING

90% of all breaches start with a phishing attack. Phishing emails are becoming more difficult to spot. Employees need to know what to look for and what to do in case they mistakenly "click the link".

13. SECURITY INFORMATION AND EVENT MANAGEMENT

Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organization's information security. SIEM tools provide: Real-time visibility across an organization's information security systems. Event log management consolidates data from numerous sources.

14. DARK WEB RESEARCH

Knowing in real-time what passwords and accounts are posted on the Dark Web allows a proactive posture toward preventing a data breach.

15. CYBER INSURANCE

If all else fails, protect your income and busines with cyber damage and recovery insurance policies.

Roark Tech Services was established in 1998. Our mission is to remain the best technology partner to our clients by doing what we do best, allowing them to focus on what they do best. Roark Tech Services navigates today's ever-evolving technology landscape to educate and provide guidance to clients so they choose the technology solutions that are best suited for their business, their budget and their future growth.

www.roarktechservices.com