SILEO
human powered cyber security

Cyber Security Roadmap

Security Audit

Hire an outside firm to do a security audit on your existing computers and network. This is the fastest way to identify your "So Very Important" data and resolve weaknesses in security. They should update and patch all operating systems, applications and firmware on every device, including printers, cameras, smartphones, tablets, laptops, servers, routers and firewalls. Have them configure your firewall to "default deny" where possible. They should also do a comprehensive check on all Known Vulnerabilities in your network. Allocate approximately 5% of your capital expenditures towards cyber security for the first year and 3% in following years. I recommend having one firm do the audit (ask your local community bank who does their audit) and a separate company to fix the actual problems – this division helps keep both sides honest.

Data Backups

It is crucial that you have an off-site, real-time, bare-metal data backup that has been test-restored and can be quickly accessed if your data is lost, destroyed or encrypted by ransomware. I use iDrive Bare Metal Recovery (BMR).

Two-Step Logins

Turn on two-factor authentication on all of your critical financial and ecommerce accounts, including banking, investments, cloud storage (Dropbox, etc.), medical, social, webmail (Gmail, etc.) and business software (Salesforce, etc.). Consider implementing two-step logins for users in your organization that have access to sensitive information.

Spam Filters

Use a 3rd-party spam detection and filtering software to help eliminate malware and phishing schemes delivered by email. Filtration is best implemented at the gateway level by your email or Internet Service Provider. Invest time upfront to train the filters properly and save all kinds of time and headaches down the road.

Password Managers

Solve the poor password habits of employees (and yourself) by implementing sophisticated and secure password management software like 1Password, Dashlane or LastPass. This eliminates most small business account takeover.

Encryption

Enable encryption on every Windows (BitLocker) or Apple (FileVault) computer that you use or ask your IT provider about enterprise-level encryption for more sophisticated security. Encrypt your mobile devices by turning passcodes on.

SILEO
human powered cyber security

Cyber Security Roadmap

Cloud Configuration

If you utilize any type of cloud-based software (from Salesforce to Facebook, Dropbox to Gmail), make sure that you or an IT expert has customized every privacy and security setting in the software and has established user-level access controls to make sure that only the necessary users can get to the sensitive data and system settings. One of the most common forms of SMB breach is facilitated by unintentional errors in configuration and authentication settings. Turn on two-step logins for every critical cloud product you utilize.

Security Software

Anti-virus and other "end-point" protection programs have lost effectiveness over years, but they are still part of the security quilt-work that will minimize the malware and phishing on your systems. I like ES|ET Endpoint Protection. I recommend installing security software on your mobile devices as well, as they are the newest gateway into your network.

Mobile Security

Switch to a longer and stronger alphanumeric password to better encrypt the data on your smartphones and tablets. Enable thumbprint biometrics on iOS devices (I don't like facial recognition for privacy reasons) and avoid biometrics on Android devices (which haven't proven as secure as Apple products). Install security software on mobile devices as well (see recommendation above). Remove all extraneous apps and keep physical possession of your device at all times.

About John

John speaks from experience – his identity was stolen and used to electronically embezzle $300,000 from his business clients. The breach destroyed John's company and consumed two years of his life as he fought to stay out of jail. Weaving his remarkable story with cutting-edge research, disarming humor and constant interaction, John inspires audiences worldwide to take ownership of the data that drives their success. John focuses on ways to make security fun and engaging, so that it sticks. Learn more about us at Sileo.com.

B.S. Training

Regularly train and entertain your employees on the latest phishing, whaling, pretexting and social engineering techniques so that they are ready with a Reflex & Response when someone is manipulating them. Teach them to Be Skeptical until the request for information has proven to be legitimate. Make security personal for themfirst. (One Shameless Plug: bring me in to speak or buy them a copy of Your Data is Showing to get them interested in Taking Security Personally :-).

Wi-Fi Protection

Internal Wi-Fi: Lock your business Wi-Fi down with WPA2+ encryption or better and MAC-specific addressing where available. Free Hotspots: When possible, utilize your cellular data connection to connect to the internet rather than free Wi-Fi hotspots (which are easily spoofed and compromised). If you need more speed, install a Virtual Private Network on all mobile devices you use to access work remotely. I have been very happy with Nord VPN for my laptop, tablet and smartphone.