TRILOGY

Seven Straightforward Cybersecurity Tips for Searchers

There are some great comprehensive cybersecurity frameworks available that over time all searchers and CEOs should have their teams embrace. Some of the ones you should expect your IT staff to be familiar with are:

- NIST (National Institute of Standards) Cybersecurity Framework: A voluntary framework primarily intended to mitigate cybersecurity risk based on existing standards, guidelines, and practices.
- CIS Critical Security Controls: A set of 20 actions designed to mitigate the threat of the majority of common cyber attacks. The controls were designed by a group of volunteer experts from a range of fields, including cyber analysts, consultants, academics, and auditors.
- ISO 270001: The international standard that describes best practice for implementing an ISMS (information security management system).
- PCI DSS: Governs the way credit and debit card information is handled. It applies to any organization (regardless of size or number of transactions) that accepts, stores, transmits or processes cardholder data.

Each of these frameworks / standards are valuable and compliance should absolutely be on your security roadmap. However, each one is a major undertaking with potentially hundreds of policies and processes needed to be in full compliance. When evaluating or purchasing the types of business most searchers will target, it is unlikely they will have the IT maturity to have implemented any of these.

So, what can you do? Here are a handful of “table stakes” precautions that every small-to-medium sized business should have implemented just to be viable in 2020. If the company you are looking at or just acquired does not have each of these seven items in place, then plan for the listed expenses to implement them ASAP.

One caveat here: these are guidelines only, and the products mentioned are just examples. If you have a solid IT staff, they probably have opinions on these things. Take this list as a discussion starter and work through the recommendations. These tips come from my experience running tech companies and interacting with a lot of CSOs, CTOs and IT specialists, but security is a moving target and will always be changing.

1 Know What Hardware the Company Owns and Where It Is.

Keep an up-to-date inventory of all of your corporate hardware. It is easy to lose track of a laptop, desktop or server. You can't secure the file server in the back closet if you don't know you own it and that it's connected to your network. Make sure you know where every device that can communicate or store data is. Are any desktops, file servers or laptops unaccounted for? Track them down and have your IT staff make a thorough and complete list and keep it up to date so you know what you need to secure.

2 Protect the Office Network

Does the corporate office firewall at each of your locations support DNS filtering for known malware and basic intrusion detection? If not, then plan on upgrading them unless the IT team has implemented a viable alternative. Some good firewall options here are WildFire from Palo Alto Networks and Firebox from Watchguard. Expect to pay $3k to $5k per device (you will want one at each corporate office) but it's worth it.

3 Patch (Update) All Your Desktops, Laptops and Servers

Keep all computers, PCs, laptops and servers patched and updated. If the vendors for your software no longer provide security updates, then find new vendors. Stuck on an old version of Windows? There is no excuse, make moving to supported versions (Windows 10) a priority. Have IT create policies so that desktops and laptops automatically update Windows or OSX. Most of the time servers should not be set to auto update for change control reasons, but do not accept leaving them unpatched for more than a week or two from when a patch comes out. Many known exploits are fixed quickly by operating system vendors but that does not help if you never update.

4 Lock Down the Corporate WiFi

Have separate guest and corporate WiFi networks. Rotate non-guest WiFi regularly. Rotate the corporate WiFi every other month or anytime an employee leaves regardless of if the employee was fired or quit. If your WiFi access points do not support separate guest and corporate accounts, upgrade them to ones that do. Ubiquity and Datto are nice corporate WiFi options starting around $500 for a small office.

5 Train Your Staff on Social Engineering

Do some basic training on social engineering, phishing and secure practices like "Don't insert that USB stick you found at the airport in your laptop". Inspired eLearning has some great ongoing courses at about $10 per employee per month. SANS has some free videos on YouTube called "Secure the Human" that are not bad. If you have IT staff, have them do regular "lunch and learn" sessions going over basic security awareness.

6 Lock Down Computers that Access Corporate Data

Convenience vs. security is always a tradeoff. There are some standard things you can do to secure your infrastructure that should not significantly impact your users.

- Password management: Require separate passwords for all key corporate assets, networks, laptops, applications. To facilitate this, provide all your employees with a password manager like LastPass or 1Password. They run from $6 a user a month to $8 a user a month. Spend the money: strong and unique passwords are too important to leave to Post-Its on monitors.
- Disk Encryption: Encrypt all corporate data on PCs and laptops. On Windows, turn on Bitlocker, on Macs turn on Filevault. This will provide an extra layer of protection in the case the device is stolen or lost and will have no noticeable effect on performance for most workloads. Both of these are included with the operating system.
- Endpoint Monitoring and Protection: The built-in antivirus software on Windows is not bad but there are better options out there that more aggressively find Malware and viruses. Ideally, you want a tool that filters malware and provides sophisticated anti-virus and anti-phishing. Some good examples are Carbon Black, WebRoot and Cylance. They augment the intrusion detection capabilities of the firewall and will help when travelling or working remotely. These will run from $30 a month per PC / laptop for Carbon Black or Webroot to $50 per device for Cylance. Volume deals are available. These tools are not cheap, but the extra layers of protection can make a huge difference with the number of threats out there.
- If you use Office 365, enroll in the Office 365 Advanced Threat Protection plan for $2 per user per month. It's an enhanced version of the free tools that come with Windows and focuses more on phishing and zero-day malware and it is worth the expense.

7 If You Have On-Premise File Servers, Test Your Backups

In tech, there is a saying that is always true: “If you have not tested your backups, you don’t have backups.” I can’t stress this enough here: regularly test your backups. Have your IT support people commit to a schedule, ideally monthly, to try to restore from backups and make sure they restore correctly with the data that you expect on each one. If possible, embrace tools like OneDrive, Google Drive or Dropbox to replace the “Documents” folder on your computers. Each of these products have free tiers for up to 2 GB and multiple computers and are great for making real time backups of non-sensitive documents and files.

These are just a few common sense tips that should not be particularly expensive or cumbersome to implement. I think they are all basic security 101 that all small to medium businesses should address.

Kevin Knoepp
Operating Executive
Trilogy Search Partners