CYBER INSIGHT

Cyber Hygiene for Small Businesses

We regularly hear the news of major data breaches perpetrated by hackers, cybercriminals, and other well-funded threat actors against large enterprises. Target. Home Depot. Equifax. The list goes on and grows daily. If these large, well-funded organizations have trouble thwarting these cyber events, how can a small or medium business expect to protect itself?

No organization is immune to these threats. Does it matter? The reason why a hacker or cybercriminal would be interested a small business varies per organization. Does the organization possess personal information which is valuable in identity theft? Does the organization do business with a larger organization which is the ultimate target, so breaching the smaller organization is just a means to an end?

With a little additional effort, there are a eight basic things that can be incorporated into your daily business practices to protect your organization. While not all encompassing, these practices will provide a foundation for an organization to protect the confidentiality of its corporate and customer data.

1. Data Classification

Most organizations cannot afford to secure all data with the same level of security. Thus, they prioritize based upon information needing protection due to the higher level of risk it poses due to loss or theft (e.g., company / customer confidential information, employee HR data, credit card information, etc.). Generally, organizations establish risk classification levels and label sensitive information according to those levels. Examples in increasing priority include: “Public”, “Internal Use Only”, “Confidential”, and “Restricted”. Doing so allows employees to ensure that sensitive information is handled according to the risk level it poses.

Not certain where to start? Focus on protecting the “crown jewel” items that fall into the “Confidential” and “Restricted” categories first, then determine what level of protections to afford to data that is not confidential.

2. Data Protection

Focus on protecting data actively being used, data when its transmitted, and data sitting at rest on computers and devices.

Data in Use: Ensure that both digital and paper media containing proprietary information is physically controlled and securely stored. Enable passwords to access computers and devices, to include setting an appropriate time out for non-use (usually 5 minutes or less). To preclude unauthorized access, lock the screen when employees walk away from the computer for a bathroom break, lunch, etc. Depending on who can view the screen, consider use of a screen privacy protector, especially if laptops are used in public places such as a coffee shop, airport, etc.

Data in Motion: Do employees just attach files with confidential information to emails a customer requests? Confidential information being sent electronically or via media (CD, DVD, USB Drive) should be protected via strong (256 bit or better) encryption. While there are lots of expensive programs to encrypt data, several commonly used office software programs support strong password protection. These include MS Office, Adobe Professional, and others. Once a password is applied, simply contact the recipient by phone or text (not via the same email system used to send the file) and provide them with the password. If using Office365 or Google, consider using One Drive or Google Drive to upload the file and send a secure link to access the file(s). Just make sure the link is configured so only the intended recipient can access the file. This method can also be used for requesting a customer to complete a form with confidential information (SSN, DOB, Credit Card data, etc.) versus just asking them to email it back to the organization.

Data at Rest: Use full disk encryption on laptops and computers. If lost or stolen, this will protect organization and customer confidential data that is on the device. All recent versions of Windows and Mac support full disk encryption. The Windows version is called BitLocker, while the Mac version is called File Vault. Make sure to back up the data prior to enabling full disk encryption. In addition, the system will provide a recovery key should the password to unencrypt be lost or forgotten. It is VERY IMPORTANT to write this down and put it in a safe place (e.g., safe deposit box or other off-site location).

3. Phishing / Web Browsing

So what is Phishing? It’s a scam that tricks an individual into revealing personal or confidential information, often via a deceptive e-mail message. It is okay to click on links when you are on trusted websites. However, when links appear in random e-mails or instant messages, THINK BEFORE YOU CLICK. Before clicking, look at the e-mail address / header. Is it from someone known and trusted – is it actually their e-mail address? Hover over the actual link – DO NOT CLICK. Does it lead to the expected website? If one does click, they are often directed to what appears to be a legitimate site asking the individual to fill in personal information or “log-in” using their credentials. Look at the browser header – is it correct? If in doubt, go directly to the original company source vs. the link that was clicked. Bottom line – avoid clicking on unknown or suspicious links.

If asked to enter confidential information on a website, look at the URL to ensure that the connection is secure (https://). Most browsers now show "secure" with a lock symbol or have a caution symbol represented by an "(!)". If the caution symbol is showing, do not enter confidential data, as the connection between the computer being used and that site is not secure and the data could be intercepted by a malicious actor.

4. Software Updates

Many of the recent cyber security breaches were made possible by a failure to install software updates when available. Regardless of whether the device being used is a PC, Mac, or smartphone, the companies manufacturing these devices provide consumers with patches to update these flaws. Get in the habit of updating regularly. This should include the basic operating system (Windows or Mac OSX), Microsoft Office Suite, web browser(s), etc. While it may seem like a hassle, investing the time to update the computers (and smartphones), could save an organization tremendous embarrassment and heartache. Do not like the idea of manually checking - enable auto updates, where available. My recommendation is to check at least weekly or when a major update is announced.

5. Hardware Disposal

Upgrading to new computers? Need a tax deduction? Why not donate those old computers (or smartphones) to a charity or other organization? Make sure all data is wiped and all settings and configurations are reset to factory defaults. Check with the manufacturer of the device for specifics on data wiping and resetting.

6. Data Shredding

All hard copy documents which contain sensitive information that is no longer needed should be shredded using a cross-cut shredder before disposal. When working from a non-company work environment (e.g., hotel, conference center, third party facility) paper copies should be protected until such time as one can appropriately destroy.

7. Password Security

A password is only good as long as it is protected. Do not write passwords down where someone can find them. Do not share passwords across multiple accounts. Even if one follows steps for creating strong passwords (12+ characters, upper case, lower case, at least one number and one special character), it can be compromised. You may protect it, but the vendor's system being using or logging into may store the password unencrypted, which is bad if their system becomes compromised. Thus, use multi-factor authentication (password, plus text, biometric, or other mechanism) whenever possible to access all accounts.

Have trouble remembering all of the passwords for all of your accounts? Consider using a password management software / application that offers credential management, multifactor authentication, a strong password generator, etc. There are several vendors out there, some better than others, and these applications make managing passwords on multiple accounts easier.

8. Training And Awareness

All of this information is only good if you or your colleagues put it to use. Make sure to document the organization's cyber security expectations. Ensure that all employees, contactors, consultants, and temporary workers are made aware of the security risks associated with their activities and that each receives and understands their responsibilities.

9. Disaster Recovery

Even with all of these controls, sometimes bad things happen. Cyber attack, fires, floods, etc. could negatively affect your business operations. Be sure to have a current (at least weekly) back-up of your critical data stored either off-site in a secure location, or securely in the cloud for disaster recovery.

Anthony Urbanovich
President

Anthony Urbanovich, President of Cyber Insight LLC, provides cyber security, privacy, governance, risk and compliance program design, implementation and management services for enterprise clients. He previously served as Chief Operating Officer for CyberGRX, Vice President, Security Assurance for American Express, Principal on Booz Allen Hamilton's commercial cyber security team, and Vice President, Privacy, Ethics, and Compliance at ChoicePoint (acquired by Lexis Nexis).

He served in the U.S. Air Force in electronic security and intelligence. He holds a B.A. in Information Systems Management from the University of Maryland, as well as CISM and CIPP/US certifications.

tony@cyberinsightllc.com
Direct: 703.624.0983