CYBERSECURITY TIPS

Cybersecurity is Crucial

Small businesses are top targets for online theft of info and funds. Ransom, extortion, skimming, spying, and outright theft are common. Incorporate basic cybersecurity management steps into your operations **today**.

Initiating Your Cybersecurity Plan

Below are ten security-first recommendations when it comes to crafting a cybersecurity plan for your business:

1) **Properly implement user training and testing** because most breaches begin with a phishing email to an unsuspecting employee. Incentives could help motivate employees to complete cybersecurity training. KnowBe4, Wizer, and Mail Fence are great options for this.

2) **Create a company procedure that requires 2nd party verification for any digital financial transaction.**

3) **Create a Rapid Incident Response Plan** that allows you to quickly call your *Cyber Incident Response Team*, notify clients, and mitigate damage.

4) **Establish Multifactor Authentication** that requires individuals to provide two or more credentials in order to authenticate their identity.

5) **Risk-based, timely patching and firewalls** help businesses secure data and protect software from vulnerabilities (outdated OSs, apps, hardware) and cybercriminals. ESET, Sophos, and Malwarebytes are great resources for anti-spam and virus firewalls. Enable encryption: BitLocker (Windows) or FileVault (Apple).

6) **Look into cyber insurance coverage options here.**

7) **Back up your important data daily** to ensure that you can easily access it in case of a data breach. Create and test an off-site, encrypted backup through iDrive / CrashPlan.

8) **Use different passphrases for each account and keep them private, unique, and strong. Consider a password manager** such as Last Pass or Kee Pass.

9) **Test your security and rate your risk** with a company such as Web Scan, Bit Sight, FICO Cyber Risk Score, or Security Scorecard.

10) **Learn more about general cybersecurity** through CIS articles or the SANS Institute's newsletters. For government contracting controls, check out NIST.

Humans Are the Weakest Link

More than 90% of cyberattacks rely on human errors. Cybercriminals often attempt to hack business infrastructure through phishing and social engineering. Establish a cybersecurity training program in your business. **Please note: it's been suggested that you can only really ask employees to change 1-2 behaviors per year. More than that can overwhelm your hard-working staff.**

Protect Business: Six Zero Cost Ideas

1. **EDUCATE YOUR STAFF!** Make sure your employees are aware of the common tricks that hackers use to deceive. KnowBe4 offers a free initial phishing attack on a business to test how vulnerable your employees are to deception. Best practices for cybersecurity posters can be found here.

2. **Take the Cyber Risk Assessment**: Knowing your risks is the first step to reducing them. From there, it becomes a risk management strategy of deciding what policies are easily changed, where you should really focus your cyber protection dollars and what can wait for a later phase. You can create a Cybersecurity Workbook here.

3. **Make a Physical Inventory**: Do you know how many laptops are in your company? Is there a smart 'sign-out' policy or another way to track their location? Always be able to quickly identify and find your electronic inventory.

4. **Update Software and Purge Unnecessary Data:** The more information you have, the more you have to lose. Frequently review and safely remove any data you don't need anymore. Extra note: Safely dispose mobile device information when you are finished with them:

   Apple IOS: Settings | General | Reset | Erase All Content
   Android: Settings | Privacy | Factory Data Reset

5. **Mobile Device Policy**: Require passwords, set lock-out timers to as short as possible, have a system for reporting and remotely wiping lost devices, set up a VPN, and don't allow personal business use on the same device. Effectively manage tethering and biometrics.

6. **Out of Sight, Out of Danger**: Establish a clean desk/workplace policy, lock up files, and keep hardware away from public areas.

To complete a free cybersecurity audit, please call Ann Swanson, Southeast Idaho SBDC Director at (208) 282-4402 or email swanann@isu.edu.

The Idaho Small Business Development Center (Idaho SBDC) is partially funded by the U.S. Small Business Administration. It operates in partnership with the SBA, Boise State University, and other funding sources. The support given by SBA through such funding does not constitute an expressed or implied endorsement of the co-sponsor's or participant's opinions, products or services. All programs are offered on a nondiscrimination basis. Reasonable accommodations for persons with disabilities will be made, if requested at least two weeks in advance. Contact Kim Sherman-Labrum, 208.426.1612. Reproduction by permission. Updated 10/5/20.