Cybersecurity for Business: Cover your Assets!

Provided by Decorah Bank & Trust Co. - October 2015

It's not news that modern technology has made business faster, and more efficient than ever before. The tech tools available today offer convenience, but with it, increasing risk. Cybercrime can be costly beyond measure. Aside from the steep monetary costs, reputational loss cannot be calculated, and can take years to rebuild. While no one is safe, utilizing some of these tips can help protect the bottom line of your workplace.

1) **Employee Training** – Employees are truly the best asset any business has, and unfortunately, are one of the biggest risks. The majority of cyber breaches occur when an employee is careless, or more often, un-informed. Regularly train your staff on basic cybersecurity principles like strong passwords, recognizing phishing, and how to respond towards suspicious activity. An educated workforce can go a long ways towards a cyber-secure business.
2) **Computer Use Policy –** Make sure you have a computer use policy in place that gives specific information on how workplace computers and other tech equipment should be used. Reviewing this policy and updating it regularly can help keep staff informed and at their best. Many businesses require employees to sign off they have read and understand it annually. It's recommended to have the IT department block websites that do not pertain to work and could be malicious. Making this policy an important piece of every new employee's orientation can set the groundwork for your expectations early, and help prevent future mishaps.
3) **Limit Employee Access –** Does every employee at your business need access to every file on the network? By limiting what each person has access to, you are forcing some dual control and making employees more accountable to each other for specific pieces of information. You are also limiting your data exposure if a device gets breached by an unwanted party or software.
4) **Mobile Device Management** – A quickly growing practice is called BYOD, or **B**ring **Y**our **O**wn **D**evice. This practice gives your employees mobility and flexibility to do business on smartphones or tablets. These mobile devices are computers too, and can be susceptible to malware, or theft. Mobile device management software gives you control over what can and cannot occur on an employee's mobile device. You should make sure all employees' devices with sensitive information have the ability to be remotely wiped and locked in the event they become lost or stolen.
5) **Not So Public Wi-Fi** – If your business offers free, open wi-fi, it may be time to look closely at how it is set up. If it can be tied into your servers where data is stored, it's time to close or hide the network. A talented hacker can gain access through wi-fi and compromise any devices connected to it. Consider securing your wi-fi with a password or hiding it from the public altogether. Train your employees to be wary of public wi-fi while traveling. Connecting in a

coffee shop may seem convenient, but not when a criminal could be watching your every move from three seats away.

6) **Corporate Card Care** – Do your employees treat your corporate payment cards with the same care they treat their own? Check with your credit card provider to ensure the same anti-fraud practices are in place on the business cards that they can offer for personal cards. Train your employees on safe credit card practices and how to keep them as secure as they can.
7) **Passwords** – This may seem like a no-brainer, but password security is still a big issue, and a common way cybercriminals breach systems. In 2014, the top two most common passwords were "password" and "123456". Make a requirement of your employees to have strong passwords, that include capital and lower case letters, numbers, and a special character like "$" or "#". Also set up your systems to require a password change at least once every six months. Utilize a secured excel sheet or password keeper software to store all your challenging passwords in one location. This way, you only need to remember one password to access all the other challenging ones you use from day to day.
8) **Insure Your Business** – Check with your insurance provider to find out if you would be covered in the event of a data breach. Take the time to discuss it with your executive team and board of directors. While the true impact of a breach is never fully known, having insurance coverage to help cover some of the losses can be well worth it. Just like your car insurance, you hope to never need to use, but are grateful for it when you do.
9) **Control Physical Access** – Breaches don't always have to occur from someone hacking into your computer. Sometimes it can be as simple as an unwanted party glancing at an employee's computer screen and quickly memorizing sensitive data. If you must have networked computers near customers, make sure employees lock the screen anytime they walk away, even if it is only for a moment. For front desk or customer facing personnel, consider getting privacy guards to place over the computer screens. These will let your employee look at the screen, but block out prying eyes from the side.
10) **Know Your Resources** – The fight against cybercrime is not on your shoulders alone. There are many resources and institutions that can help. The Department of Homeland Security and the FBI both have websites with the latest information and additional tips to help stay secure. Your local bank (like Decorah Bank & Trust) can help answer questions on transactions and online banking and give you advice on keeping your financial information safe.

It's important to remember cybercriminals will often go after the easiest targets. Some basic security steps, employee education, and vigilant monitoring can help protect your business from cybercrime and data breaches. The harder you make it to be breached, the more successful you will be.