Volume 26, Issue 1

Page 1

MICRODATA

Micro/Outlook

Cyber Security Guide for Small Business

I've written on many IT security topics over the years, so I thought I'd start off 2018 by putting together a collection of my best advice for business. These are the things that, were our positions reversed, I'd want someone to tell me. And while not an exhaustive listing, if your business can implement the strategies I'm sharing here this month, you'll be 90% ahead of everyone else. And if you have colleagues that you think could benefit from this guide, share a copy of this issue with them or email us with their contact info at ask@microdata.com and we'll forward them a free copy.

To begin, we need to make an honest assessment of the reality of today's IT threats and why they require a

different response than a few years ago.

First, it's important to understand that Cybercrime is big business being driven by sophisticated criminal enterprises and not some teenager in their parent's

Continued on pg 2

MicroData SecureCloud: 30-Day Free Trial and your 1st Month Free!

MicroData *SecureCloud* does two things. It provides **automatic, secure, and continuous file sync** in the Cloud. It also can provide a **simple, automatic Cloud backup** of critical data from a server or PC/Mac.

Sound a little like DropBox for Business? It is similar but it has some important features that DropBox doesn't offer. Specifically File Server Enablement, single click version rollback (solves ransomware attacks), and Active Directory integration.

30-day free trials are available! And your 1st month of service is free if ordered by Feb 15.

Learn more at microdata.com/backup

It's our 26th year!

It's hard to believe but MicroData turns 26 this year. When we started out Novell Netware was the only real small business network operating system, CAT5 data wiring hadn't been invented, email and the Internet didn't exist, and a 56K modem was considered 'high end' for connectivity.

We've come a long way since and I'd like to thanks all our customers, partners, and employees who have been on the journey with us. We're looking forward to many more years!

-Glenn

Inside this issue:

January 2018

This monthly publication is provided courtesy of Glenn Mores, President & CEO of MicroData of Beverly Massachusetts.

Our Mission: To Provide Phenomenal IT Support to companies throughout the Eastern Massachusetts/Southern NH area.

Cyber Security Guide for Small Business, continued

basement. According to the just-released *Norton Cyber Security's 2017* insights report, cybercrime victims collectively lost $172 billion last year. And 32 percent of all cybercrimes were initiated by phishing attacks – an attack vector that didn't even exist a few years ago.

And consider the Equifax data breach. 143 million records were compromised. And this wasn't just one person stealing a credit card, this was a small group of cybercriminals that stole HALF of the U.S. population's data in one fell swoop.

> ...cybercrime victims collectively lost $172 billion last year

Second, don't think "I'm just a small business. I'm not Target or J.P Morgan, so nobody would want to hack us." WRONG. Those large businesses have big IT staffs and budgets and are a much harder target to penetrate. Cybercriminals know that small businesses are much easier to rob. Sure, the prize isn't as big but there are many, many more small businesses than Fortune 1000's.

So what should you do **right now** to help protect your business?

Deploy a solid and unified threat management solution. Most companies put security safeguards into place when they deploy the underlying asset or technology. This creates a patchwork collection of tools that usually don't work together, get out of date, and often miss important new security areas.

Implement Spam Filtering. If you don't already have spam filtering for whatever email solution you use, add it now. Cybercriminals know it's far easier to trick your employees into helping them than it is to break through a firewall. And with spam filtering only costing a few dollars a month, there's no reason not to have a good quality solution in place.

Control what website employees are accessing. Breaches commonly occur when employees browse to websites that have infected content. On such a site, you don't even need to click on anything to get infected.

Lock down the use of 3rd party apps. Webmail, DropBox, and other low-cost or free services are a major security risk as they can effectively bypass all the security measures you put into place.

Force Complex Passwords. I know it's a pain, but there's just no excuse any longer for setting your password to "password" or something equally ridiculous. And require passwords to be changed every 45-60 days or immediately after a key employee leaves.

Restrict users ability to install software without your knowledge. Keyloggers, ransomware, and similar cybercrime tools are all software. So by restricting a system's ability to install the software, you can head off the damage caused even if an employee makes a mistake and clicks somewhere they shouldn't have.

Back up your systems properly. I can't tell you how many times we've responded to a disaster only to find that the backups either weren't working or were only backing up some of the data. The $19 month *Carbonite* backup won't do it, so get some help from an IT pro.

Employee Education and an Acceptable Use Policy. Cybercriminals have figured out that people are the weakest link in the cybersecurity chain, so get your employees educated. No technology in the world can 100% prevent an employee from falling for a sophisticated phishing attack, so training is the solution. We recommend KnowBe4's *Security Awareness Training*. And create an AUP and go over it with your employees so they really understand how important these issues are and what's expected.

Keep systems updated. Do you remember the *WannaCry* ransomware from this past summer? It worked by exploiting a bug in Windows, but before you start criticizing Microsoft, they released a fix for the bug quite a few months prior. So there was really no good reason any organization should have been hit.

I hope these tips help you and your business. And of course we'd be glad to assist your company with Cyber Security. We have tools to rapidly and efficiently implement all these policies.

-Glenn Mores

You can contact MicroData with any questions or for assistance with IT issues at 800.924.8167. Or visit us on the web at www.microdata.com

Hardware Find of the Month

HP EliteDisplay E243, $169

Save your eyes with the HP EliteDisplay 23.8" full HD monitor.

1920x1080 resolution with a 23.8"IPS screen. Modern and energy efficient.

To order contact us at 800.924.8167. Shipping additional or may be picked up at our offices in Beverly.

How to Choose a Mentor

The benefits of having a mentor are big. A survey of Fortune 500 companies found that 96% of executives credited mentoring as an important development tool and 75% said mentoring played a key role in their career success.

But how do you get a mentor?

Many employees and managers complain about not having a mentor. Such people are usually waiting for the company to assign a mentor to them. Mentoring works much better when the mentee takes responsibility for choosing a mentor.

So, the first place to start is to find one yourself! Below are some characteristics of great mentors:

Respect: Look for someone that others respect. A mentor should be someone who can be looked up to as a role model of the company's values and ideals and who understands the culture of the organization, its practices and the strategies needed to negotiate them. Additionally, it should be someone that you want to assist you in planning and achieving your career goals.

Broccoli Pointer: A mentor is someone who is capable of pointing out embarrassing things about how you are "showing up" at work. Think of it this way, if you came back from lunch with broccoli in your teeth, a mentor wouldn't be shy about pointing it out!

Independent Loyalist: While a mentor is someone who is loyal to the company, he shouldn't have drunken so much of the organizational happy-juice that he can't think independently. Pick a mentor who has a mind of his or her own.

There for You: Find a mentor who will be available to meet with you regularly. Regular meetings will help to not only build a relationship, but will also enable you and your mentee to address topics on an on-going basis. Create a schedule. Consider meeting every month or two (sooner if you're experiencing particularly tough work challenges).

Expert in Their Field: Your mentor should have job-related expertise in the field in which you wish to grow. This might be technological or managerial. It is expertise that you may find useful in their current or future roles.

Storytellers: A great mentor is a master storyteller. When you're struggling with an issue, your mentor should willingly share a story about a similar struggle that he faced in the past.

Lifelong Learner: Experience accumulated through the mentor's own life of personal issues that are or are likely to be of particular use to the person being mentored. Pick a mentor who constantly strives to be a better leader himself. Ask the mentor who he or she considers to be his or her mentor(s).

The aim of mentoring is to build the capability of you, the mentee. As such, you should always choose a mentor who you feel can respond to your needs in a way that enables you to find your own solutions to problems that you may be dealing with. Ultimately, your mentor should help build you up to eventually have a mentee of your own!

Bill Treasurer is the Founder & Chief Encouragement Officer at Giant Leap Consulting, a courage-building company that exists to help people and organizations live more courageously. Bill's newest book, Leaders Open Doors, focuses on the responsibility that leaders have for providing people with opportunities that cause them to grow and develop. Notably, Treasurer is donating 100% of the royalties to programs that support children with special needs. Learn more at www.http://giantleapconsulting.com/

Client Spotlight: Meadowbrook Golf Club

Meadow Brook came to MicroData with a variety of problems with their network that served the administrative operation as well as their restaurant and Pro Shop. Performance was so bad that online accounting tasks could literally take minutes per transaction.

MicroData performed an audit of the existing network, crafted a design to correct the problems, then executed a plan for a Hybrid-Cloud solution.

"MicroData drastically improved network performance, speed, uptime, security, and my peace-of-mind; they also replaced our older POS terminals and worked with our application vendor to ensure complete success."

- Bob Morelli, General Manager.

Would you like your company highlighted here in our 'Client Spotlight'? Give us a call today at

Tech Tips

Keeping Web Passwords out of the Hands of Hackers

OK, so you have a website that either your employees or customers access to do business with you. What do you need to do in order to keep information collected on the site safe?

Secure Your Website

Many password thefts start with an attack on the company's website. Before you go live have your site checked by a security expert for software vulnerabilities or coding errors that open paths to your database.

Store Passwords Safely

Make sure your passwords are strongly encrypted making it difficult or impossible for someone whose trying to get in. Companies should "hash" passwords using encryption technology or adding random data to the password making it even more complicated for

someone to guess.

Consider Two-Factor Authentication

First it requires something you know and something you have in your possession. Second is a device that provides difficult -to-steal, one-time code that users enter along with their password.

Google has begun to allow businesses to use OpenID to connect to the system for free to get authentication which includes the 2-step verification with a text message. Companies can do the same but it is called Google Authenticator.

If your password unlocks sensitive information you should consider implementing this two-factor authentication.

Put It In Writing and Identify

When hiring a web developer you should include password security in your requirements so they will have to fix any problems. Make sure any third -party software you use has a secure password arrangement.

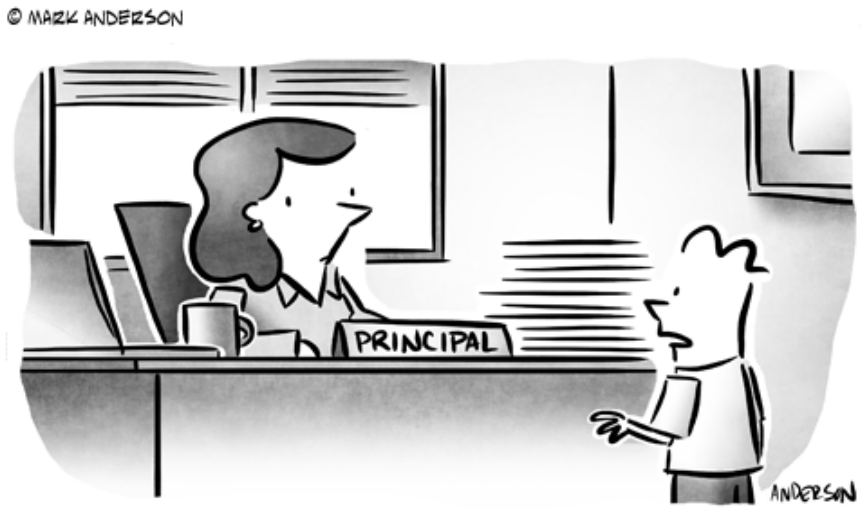
Suggestion: Address the top 10 web application security risks identified by the non-profit group OWASP which includes insecure password storage.

Monitor Your Site

Don't just set it and forget it! Any device that is on the Internet is a target of automated bots that try to locate and exploit vulnerabilities, 24x7x365.

Keep Your Site Updated

Closely related to monitoring is the need to keep your site—and all the software libraries and components that make it work—up to date. Patches and fixes are released specifically to fix vulnerabilities so don't leave this easy door open for cybercriminals to exploit.



"You know, in the tech world being disruptive is seen as a positive."

MicroData
100 Cummings Center, Ste 146N
Beverly, MA 01915
978.921.0990
www.microdata.com
www.facebook.com/microdata
www.twitter.com/microdatait