It's Time to *Really* Start Talking Cybersecurity

At the risk of sounding like Chicken Little (you know the one who runs around talking about the sky falling) the current global "go-ings on" are the closest we'll ever get to advanced warning that cybersecurity is something every business needs to worry about. Big or small, selling globally or just in your tiny town, if you do anything online, your data is in (potential) jeopardy.

Here are the things you need to do now. Seriously.

Invest in Protection

While there are many articles out there that will tell you small ways businesses are at risk, it's important to know that cybersecurity is something you will now have to consider as part of your business' annual budget. Running updates as soon as they come out isn't enough protection. Storing data in the cloud, isn't enough if those cloud companies get hacked. Making sure your virus protection is in place…while all these things are good, they aren't enough anymore.

You need to speak with a cybersecurity expert. Rest assured a good expert will offer a customized plan for your business and work within your budget. But cybersecurity is now something you will have to budget for as a line item. Move toward that now.

Don't Ignore Warnings

The Cybersecurity and Infrastructure Security Agency (CISA) and FBI have issued warnings over the past two months about the imminent threats of destructive malware aimed at organizations with dealings in the Ukraine. However, the agencies believe it is only a matter of time before American businesses (with no connections to that area of the world) are targeted too.

The actions that CISA/FBI urge companies to act on as soon as possible (meaning today, start these things today) include:

- Set antivirus and antimalware programs to conduct regular scans.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Filter network traffic.
- Update software.
- Require multifactor authentication.

- Use strong passwords, single use only (not the same ones across every site you access), and change them often. Set your machines to require it.
- Regularly backup data offline. Yes, a few years ago we were told cloud was everything. Now we stress redundancies. Do both.
- Implement network segmentation. You don't want to give access to everything through one "door."
- Work with a professional to draft a recovery plan.
- Require credentials to install software.
- Configure access controls with "least privilege" in mind. If your employee doesn't need it, don't give them access.
- Consider a VPN. Over the last several years, it's become increasingly easy to access machines and log in to work from home. It was essential to work during COVID. But now that easy access can cause big problems.
- Disable hyperlinks in emails.
- Train your employees on cybersecurity and potential threats. Even savvy employees can be tricked by coincidences. For instance, an email from "Federal Express" when they're expecting a package can cause a lapse in judgment. While they may not normally click on something suspect like an attachment in an email, in this example it seemed legitimate because it fit into their world/expectations at that moment.

If you're not sure where to turn to start working on these things—and you don't have an IT department—check with your local chamber. They often know of resources in the area and cybersecurity experts who can walk you through what you need to know. Also, read the Cyber Essential Resources for Small Business from CISA. It will help you decide where to start and how to begin cyber security implementation to keep you and your customers safe.

Don't wait for something terrible to befall your organization (and this goes for nonprofits, too. Your lists could be very valuable). If you conduct any sort of business online or have any lists or data on your computer or in the cloud, you need to investigate the necessary level of protection and begin a plan for implementation. Once malware strikes, even large companies with huge budgets are helpless.

This is a business threat that you need to be proactive about. Being reactive to this threat is the same as doing nothing and that just won't do.

obp | Positively Oberlin!

Christina R. Metcalf (formerly Green) is a marketer who enjoys using the power of story and refuses to believe meaningful copy can be written by bots. She helps chamber and small business professionals find the right words when they don't have the time or interest to do so.