BERTIGROUP
MANAGED IT SERVICES

BERTIBRIEF

Issue #19- February 2020

In This Issue

If You Think Your Business Is Too Small To Be Hacked … You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank cheques. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security, but it isn't set up correctly. At the same time, cybercriminals send emails to businesses (and all the employees) with links to phishing websites or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. Cont'd Page 3…

TOP TIPS FOR SCALING SECURITY FOR YOUR SMALL BUSINESS

Put a greater emphasis on passwords. As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single licence for a piece of software, which means they share a single password. Password managers like LastPass or IT Glue can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA). MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the log-in process. But an extra 15 seconds to log in is worth it for the security. There are many MFA options available for different-sized businesses. Make it a part of your cyber security policy.

Small Business Trends, Nov. 1, 2019.

3 Reasons Why Recessions Are Awesome For Great Companies

It may be jarring to read the words "recession" and "awesome" in the same sentence. Recessions are bad for most people. I will not make light of how horrible recessions are for the vast majority of companies and their employees (as well as for not-for-profit organizations and governments).

For most companies, recessions mean increased stress at work, stalled career progression or even layoffs, uncertainty, increased board and shareholder pressure, increased financial strain and a feeling of looming danger in the pit of your stomach, which is no fun to wake up to every day!

But for great companies, recessions can be awesome.

What are great companies?

Great companies make great products or deliver great services to customers. They provide a wonderful work culture that attracts and retains talented people. And because they take great care of customers and employees, great companies don't have a dangerous debt burden. But you must be wondering, how are recessions awesome for great companies?

Recessions allow great companies an opportunity to do the following:

1. Shake loose the cobwebs of complacency.

"Success breeds complacency," said Andy Grove, the legendary CEO of Intel. And while I'm not here to suggest everybody embrace full-on "paranoia" in the workplace (Only The Paranoid Survive), I am here to suggest that great companies have to keep hustling to stay great. A recession provides an opportunity for a wake-up call to great companies that may start to coast on past greatness and help them get back on track.

2. Take customers and colleagues away from lesser companies that don't deserve them. As lesser companies stumble during recession (e.g., shutting locations, letting service and quality drop, highlighting dysfunction in the culture, etc.), it's the perfect time for great companies to pick up more customers and talented people. I remember when a successful business services company with 70 locations around North America entered the '08 recession. Lesser competitors were closing branches and laying off people, and service was slipping. But the CEO of the successful company was not fearful about the recession. Instead, he sensed the opportunity to win more customers with better service and poach some top talent away from the struggling competitors. The recession allowed this great company to gain market share and build a stronger leadership talent pipeline. Cont'd page 4 …

7 Things To Do So You DON'T Get Hacked When Shopping Online

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any email you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favourite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. Lifehacker, Nov. 19, 2019.

They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. Many business owners fall into the habit of complacency, thinking if "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."Cybercriminals don't think like this. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk.The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be having the cyber security talk right from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security is a great way to build and maintain trust with these people. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to us we will do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

Impact of Social Media On Security And Employee Productivity

If you are business owner concerned about employees wasting time online using non-work-related web sites like Facebook or Twitter -OR WORSE, using company resources to access gambling sites, hate groups, or more ?

Why You Should Be Concerned ?

While it's not uncommon for employees to waste a bit of work time on relatively harmless activities such as shopping or visiting a favourite sport site, times have changed; employers are learning the hard way that employees use or abuse of a company's internet system can lead to a significant liability and time wasted if not monitored.

Social media sites Twitter and Facebook are addictive, if your employees are constantly "plugged in" to those sites, they won't be nearly as productive at work as they should be.

How To Solve This Problem

Protecting your company requires two simple steps at minimum. The first is to have a written company policy that details what employee can or cannot do with company resources or during company hours.Next, you'll want to have a content filtering system in place that will enforce your policy by automatically "policing" your company e-mail and Internet usage, blocking sites and content you don't want your employees to access without hindering their ability to work online.

At Berti Group we have a content filtering software that monitors such activity and then provide a report of how much time is spent on non-work related content browsing while at work, shoot us an email ask@bertigroup.com to find out more about this service.

3. Increase the rate of learning of your leaders.

Time seems to move more quickly for me during harder times than during easy times. This can improve the learning curve of your up-and-coming leaders. Just remember to not make too many decisions for them; that will stunt their growth. Allow your leaders to come to you with problems and solutions, and coach and support them. Let them test and learn various approaches to leading through uncertain times.

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book Who: A Method For Hiring and the author of the No. 1 Wall Street Journal best seller Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honours from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

Client of The Month- Innocept

Our Client of the Month is **Innocept Development & Real Estate Outsourcing**. A full-service boutique real estate outsourcing firm, that specializes in tenant representation, project development/ management and real estate consulting. As an organization that is involved in real- estate, they are highly devoted to building long-standing relationships and their client's best interests. Innocept has a wide roster of current and former clients such as from Kit and Ace, Gold's Gym, Rexall, Sobeys, Sport Check, Good Earth, Canadian Tire, are some to name.

Innocept came to us through Consultants' Network and they are utilizing all the benefits of a BertiCare Diamond Plan. Upon inquiring about their experience so far with Berti Group, they have nothing but good to say about us. They believe that moving to a BertiCare plan, has empowered them with an external IT department that is quick to respond and flexible to accommodate urgent needs, they are impressed with our friendly and attentive staff that resolves their issues on regular basis. Innocept suggests that if someone is on the fence to pick Berti Group as their IT company, their suggestion to them would not be reluctant in switching, but if you never do, you may never experience the superior levels of service that Berti Group has to offer. We are excited about this partnership and our goal is to continue to exceed their expectations in the future while providing them with excellent IT solutions.