TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Stop Cybercriminals and Security Breaches In Their Tracks

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You were set. But then you forgot to do one crucial thing: you didn't stay up-to- date with your IT security policy. This is a trap countless businesses fall into. They invest in great cyber security once. Five years ago, this was fantastic. The problem is that cyberthreats are constantly evolving. Methods used by hackers and cybercriminals have come a long way in the past five years. Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense. What can you do to stay up-to-date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand The Threats
It's easy to assume that hackers are trying to get into your network the "old-fashioned" way. You might picture them hacking your network trying to get your passwords and usernames or breaking through your firewall protection. While some hackers will do this (it's easy for them if you use simple passwords), many of today's cybercriminals rely on social engineering. The most common form of social engineering is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file.

WHAT'S NEW INSIDE KAMIND IT

With July comes the addition of a new team member to KAMIND IT. Please help us welcome **Doug Key** as our new **Operations Manager!**

Our Creative Director, Jack Biehn has purchased **a Great Dane Puppy named Hades**. Help us in welcoming Hades to **KAMIND & Jack's Family.**

KAMIND IT has recieved their 6th Microsoft Gold Certification. KAMIND IT always Improving the way we assist our clients!

3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

Continued from page one

Cybercriminals have gotten VERY sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people. This is why you need a cyber security handbook – one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And Update

From software to hardware, you must stay updated. There is no such thing as "one-and-done" when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated. Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them. What happens when a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software. You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated and keep all your devices and software UPDATED!

Invest In Proactive Network Monitoring

When it comes to the security of your network and overall business, being proactive can make a huge difference. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped. The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want
updates once a day or once a week? That can be done too! This approach means you have one less thing to think about. Someone is always keeping an eye on your network, making sure the bad guys stay out. You might think, "How am I going to do all this?"

You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will be updated on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

Building Confidence As A Business Leader

How can you build your confidence as a CEO, investor or entrepreneur? My colleagues and I at ghSMART see many talented people work hard to build their confidence. New CEOs have imposter syndrome. Private equity investors who just raised another $1 billion in funds read newspaper headlines about the coming recession and quietly gulp. Self-made billionaire entrepreneurs worry that their fortunes will take an embarrassing hit. Newly elected government leaders worry about whether their results will live up to their campaign promises.

We find that leaders are less confident when they obsess about things they can't control, rather than take action in the areas they can control.

Like what?
The Wall Street Journal reported the results of a Conference Board survey (Jan. 16, 2019) of what is on the mind of 800 CEOs.

External Hot-Button Issues
- Recession
- Global trade
- Politics

Internal Hot-Button Issues
- Attracting and retaining top talent
- Disruptive technologies
- Developing the next generation of leaders

What this survey says to me is this: it's good to be aware of issues that are outside of your control – recession, global trade and politics. But it's even more brilliant to master the things that are within your control – hiring and retaining top talent, developing digital capabilities and developing the next generation of leaders.

How much confidence do you have in your team?
If you have a high degree of confidence in your team, then keep doing what you are doing to hire and develop them. But if you don't have a high degree of confidence in your team, then you should focus on hiring, developing and retaining more of the right people who fit your strategy and who can achieve the results you seek.

How?
There are three ways to build confidence in your team. You can invest the time to master the skills and best practices around hiring, developing and retaining top talent yourself.
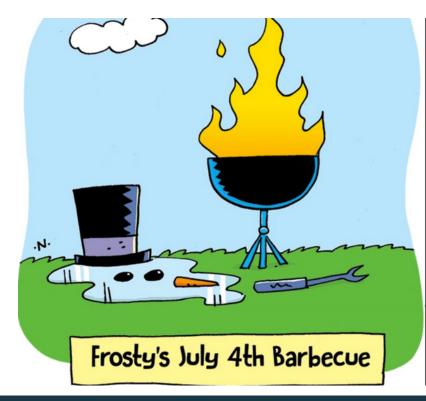
You can engage ghSMART to do it for you. Or (what most of our clients do) you can engage ghSMART to solve this problem immediately and build your skills in this area for your long-term success. (A quick side note: I'm very proud to report that my colleagues achieved 99% "high" client-reported satisfaction over the past 12 months. So, to go with this confidence theme, I have a very high degree of confidence that my team will help you solve your #1 problem!)

A great way to build confidence in yourself as a leader is to build your confidence in your team.
If you are the CEO of a company that generates over $1 billion in revenue (or has raised at least a $1 billion fund), then please reach out if you would like my team to help you build confidence in your team to deliver the results you want to achieve for customers, employees and shareholders.

Author:
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 ProgramTM** provides 10 years of leadership tutoring, and the **Leaders InitiativeTM** seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.

Frosty's July 4th Barbecue

3 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly
and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible.

Inc., July 30, 2019

How Malware Can Cripple Your Business

Every year, the number of malware attacks on small businesses increases. Semantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%. The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more. In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people. If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late.

Small Business Trends, Oct. 12, 2019

Small Business Data Breaches in 2020

With small businesses making up 28% of the breaches, owners have to be more proactive in protecting their digital presence. Whether it is an eCommerce site, blog, V-log, podcast, or other digital assets, you have to protect your domain. This not only ensures your data is safe, but it is one more tool you can use to attract new customers; robust security.

The Danger to Small Business

With that in mind, how are small businesses attacked in 2020? According to DBIR, the dividing line between small and large businesses is smaller today. The report attributes this to the movement toward the cloud and its numerous web-based tools, as well as the continued rise of social attacks. This has led the criminals to alter their forms of attack to get the information they need in the quickest and easiest way.

This monthly publication is provided courtesy of **Matt Katzer, CEO of KAMIND IT** & Amazon Best-Selling Author of *"Securing Office 365 - Masterminding MDM and Compliance In The Cloud"*

KAMIND IT's Mission: "KAMIND IT Assists Organizations to Utilize Technology to Drive Innovation"