

On Thin Ice:

How Just ONE Cyber Attack Can Put Your Business And Finances UNDERWATER ...

And What YOU Can Do NOW To Stop It

By Tim Nyberg

You've probably read about the multimillion dollar data breaches of Home Depot, Uber, Capital One and more. While cyber attacks of global companies make the headlines, fact is that most cybercriminals target small businesses like YOURS. Why? Small businesses don't typically have the security and safeguards in place to protect their data. It's easy prey.

Not so fast! The Amazon Best Selling book titled *On Thin Ice: How Just ONE Cyber Attack Can Put Your Business And Finances UNDERWATER ... And What YOU Can Do NOW To Stop It*, co-authored by **Tim Nyberg** from **The MacGuys+**, gives businesses like yours the knowledge, strategies and action steps to protect your data and business from hackers.



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

December 2020



This monthly publication provided courtesy of Tim Nyberg, President of The MacGuys+

Brand Promise:

The MacGuys+ provides proactive support, maintenance, and alerts from certified Mac experts that combines friendly, accessible advice with honesty and integrity, so Mac owners can stay online and productive, keep their personal information secure, and realize the limitless potential of their Mac devices.

Did you know the average website is attacked 94 times every day? As cybercriminals become better equipped with more advanced technology, that number will increase. Small-business websites (and small businesses, in general) are the most at risk for attack. Small businesses are tempting targets because SMB websites are often a direct link to that SMB's network, where all kinds of goodies are stored, including sensitive business and customer data.

This is data cybercriminals want.

Cybercriminals and hackers can be aggressive when it comes to attempting to access your network and data. They use malware,

ransomware, phishing scams, bot attacks and even direct attacks to get to your data. If you don't have protections in place against these kinds of incursions, you are putting your business in harm's way.

There are many "barriers" you can put between your business and the bad guys, but there are four things you can do (and should do) **right now** to put yourself ahead of the curve. These will protect your business and protect your data.

- 1. Create A Culture Of Awareness.** Education is a powerful tool, and that

Continued on Page 2 ...

... continued from Cover

is 100% true when it comes to cyber security. There are several steps you can take to create a culture of awareness. This includes employee cyber security training, along with ongoing education that keeps everyone in your organization informed about the latest threats and the latest ways to combat those threats.

Training helps your team identify threats and recognize when someone is trying to break into your network (such as through a phishing scam). Because cyber threats are constantly evolving, ongoing education will keep these threats top of mind, so as the threats change, your team is right there on the frontlines ready to take on whatever may be around the corner.

2. Monitor Threats 24/7. This is where partnering with an experienced IT services firm really comes in handy. Coming back to point #1, an IT services company can help you create

“You should have an IT handbook – a plan that spells out every detail of your IT protocol and cyber security strategies.”

that culture of awareness, but more than that, they can keep two eyes on your network 24/7. This way, if something or someone attempts to force their way into your network, they can stop it before it becomes a problem.

Even better, threat monitoring helps protect your team from more common types of attacks, such as malware or ransomware attacks. Should an employee accidentally click a harmful link or download a malicious program, it can be isolated before it takes hold and spreads.

3. Make Sure Protections Are Up-To-Date. Practically every piece of hardware and software you use needs to be updated at some point. When you don't update, you put yourself at serious risk. Hackers are constantly looking for vulnerabilities in the apps and devices you use. CRM software is a good example. This software connects your business with customers, and it can be used to store all kinds of information, from very basic contact information to very sensitive customer-specific data.

Should a vulnerability be found, hackers won't waste any time attempting to exploit it. In response, the makers of that CRM software should send out a security patch. If you do not make the update (or have the update automatically installed), your risk increases significantly.

Again, working with an IT services firm or a managed services provider can help you

address this minor – but very important – step. They can ensure everything under your roof is up-to-date and that you have all the latest protections.

4. Have A Plan. Every single person on your team should be on the same page. They should all change their passwords every 60–90 days. They should all be required to use secure passwords. They should know how to identify potential phishing scams. They should know who to call if the network or their devices go down for any reason. You should know exactly what to do if your on-site data becomes compromised in any way, whether it's due to malware, a natural disaster (flooding, fire, etc.) or hardware failure.

In short, you should have an IT handbook – a plan that spells out every detail of your IT protocol and cyber security strategies. This goes hand in hand with the three points we've already discussed: awareness, threat monitoring and keeping hardware and software updated. When you have a plan, you know **exactly** what to do when threats come your way. You're ready and aware.

Cyber threats are always going to be out there. There isn't anything you can do about that. But there are things you can do for yourself and your business to prepare for those threats. Put these four points into action, work with an IT services provider and give yourself the advantage over those who want to take advantage.

The Top 11 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are “low hanging fruit.” Don't be their next victim! This report reveals the most common ways that hackers get in and how to protect yourself today.

In this free executive brief, we cover:

- ✓ The #1 threat to your business that even the BEST firewalls and anti-virus software can't protect against (and what you need to do now to remedy it).
- ✓ A common misconception about employee devices on your office network and exactly what you need to do now to shut this down immediately.
- ✓ The shocking facts about why small business are the #1 target of cybercriminals - more than half of the reported cyber attacks are focused on small business for this one main reason that is easily fixed.
- ✓ How to keep your network secure with the proliferation of mobile devices, cloud applications, e-mail, and social media sites connecting to your computer network.



To Download Your Free Copy Today, go to themacguys.com/11ways Or Give Us A Call At 763-331-6227

Offer valid only for business offices in The Twin Cities Metro with 5 or more Macs.

Cartoon Of The Month



“I've never heard of this Oz. And you say a wizard gave you this diploma?”

... continued from Page 4

- **Evaluate The Market And Cut Costs.** Recognizing how customer needs are shifting is especially useful during economic distress. Cutting costs is equally important because choosing which revenue stream to monetize should intersect with the services you provide.
- **Stay True To Yourself As Much As Possible.** Don't stray too far from your core business — focus on what you do well and how you add value to your customers' lives. There's such a thing as overdiversifying.
- **Invest In Digital Updates And A Diverse Team.** Technology can help companies shift models to meet customer needs and generate revenue. Coupling that with a diverse workforce full of different perspectives can lead to winning ideas. *Business Insider*, Sept. 24, 2020

A Warning About Using Bluetooth Devices



We all know using WiFi comes with risks, especially unsecured public WiFi. But what about your device's wireless Bluetooth connection? Many devices use Bluetooth as a way to pair with other devices (like smartphones to wireless earbuds). However, recent hacks highlight the danger that comes with Bluetooth.

One example is called BLES (Bluetooth Low Energy Spoofing Attack), which targets devices using Bluetooth Low Energy (BLE) protocol, a technology common in smartphones. It allows hackers to trick Bluetooth-enabled devices into thinking they're another Bluetooth device, giving them access to the phone. Using Bluetooth comes with risks. If you aren't **actively** paired with another device, it should **always be turned off**.

The 2 Secrets To World-Class Service – It's Not What You Think

Nick Stoyer, Learning and Development Leader at Four Seasons Resort Orlando, revealed some secrets to world-class service. Nick was generous enough to stop off at our summit to share some secrets to success, and he and his firm agreed to allow us to share them with you.

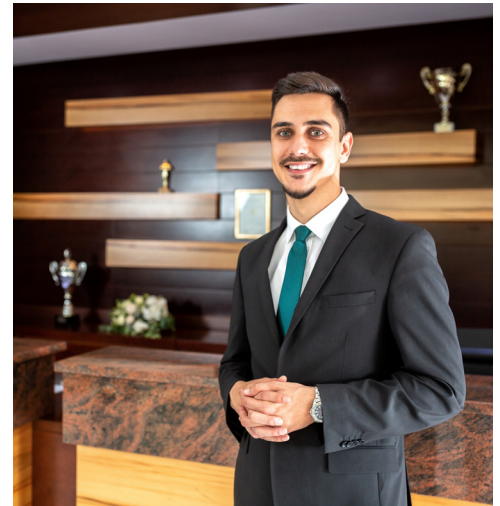
How does the Four Seasons deliver world-class service across the globe? That was the central question. Below are some excerpts from the conversation. I hope you find the insights as powerful and as useful as we did.

Geoff: Four Seasons Hotels and Resorts is known as the gold standard for service worldwide. It has achieved more *Forbes* five-star ratings than any other hotel and resort brand in the world, among a long list of “best of” awards. The experience is unique, and it's consistently awesome. Any company in any industry can benefit from learning from your example. The question is, “**How do you do that?**”

Nick: Long before it was fashionable for CEOs to talk about doing good in the world and treating “stakeholders” (also known as “people”) well, Four Seasons was practicing the Golden Rule: to treat others as you wish to be treated. Our founder, Issy Sharp, son of Polish immigrants, started Four Seasons in 1961 in Toronto. It seemed to him that if you wanted to build the best hospitality company in the world, you had to treat your colleagues and guests the best.

Geoff: Easier said than done.

Nick: For us, it's all about the people we hire, the way we develop them and the culture we build together. That's what we focus on in order to give our guests the best possible



experience. One of our guests said that she defines luxury as “the absence of worry.” We thought it was brilliant, and we rolled it out as our definition of luxury. So, we need to hire the best people, develop them and give them a culture of support (alleviating them of worry as a team member), so they can do their best to free our guests from worry.

Geoff: Beyond developing and coaching people, what's the culture like at Four Seasons?

Nick: It's very positive, even in failure. We have this saying: “You either win or you learn something.” Everything we do, we try to make it as fun and engaging as it can be. We innovate constantly. We are building micro-videos of best practices. We constantly huddle and talk about if a guest or a colleague needs something special. That's the culture. It's one of overwhelming support and encouragement. This permits our folks to really focus on the guests, observe what they need and take action.



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 #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 Bachelor of Arts in Economics with honors from Northwestern University and a Master's and Doctorate in Psychology from Claremont Graduate University.



1650 West End Blvd, Suite 100
St. Louis Park, MN 55416



Critical Cyber Security Protections EVERY
Business Must Have In Place NOW | 1

The Top 11 Ways Hackers Get
Around Your Firewall And Anti-Virus
To Rob You Blind | 2

The 2 Secrets To World-Class Service – It's
Not What You Think | 3

Rejuvenate Your E-mails, Sales And Revenue Streams

4 STRATEGIES TO IMPROVE E-MAIL PRODUCTIVITY

As work situations have gone remote, e-mail has become even more vital for communication. So make sure your e-mail habits are good.

- **Rethink Your Subject Line.** Tell the recipient as much as possible in as few words as manageable and make sure to let the recipient know if any action is needed on their part.
- **Establish Addressing Rules.** It's annoying to be copied on an endless series of e-mail replies. Establish team rules about who needs to pay attention to which e-mails by properly utilizing the "To" and "CC" fields.
- **Use Caution When BCC-ing.** Blind copying people on e-mails comes across as sneaky. Refrain from it as much as possible. Only use it for bulk e-mails or

when you want to politely drop someone from a chain they no longer need.

- **Don't Draw Things Out.** If you can't resolve something in three e-mails or less, it's time to pick up the phone. Sometimes e-mail just doesn't work.

SALES CONTEST IDEAS TO MOTIVATE YOUR TEAM

If you want to make more sales, you have to motivate your team to do so. Here are some ways to incentivize great work.

- **Raffle Prizes.** Each salesperson receives raffle tickets for every sale or other objective they reach, and at the end of the month, you can hold a raffle for prizes.
- **Sales Madness.** As you do with March Madness, set up a bracket for your sales staff. Whoever has the most sales at the end of a set window moves onto the next round, working their way toward a prize.

- **Conversion Contest.**

This is a great way to give everyone the same opportunity to win, no matter their sales history. Distribute new leads evenly and reward the person who converts the most sales.

- **Slump-Buster Contest.** When business is slow, challenge your team to contact old or existing customers to sell repeat or upgraded products.

TOP WAYS TO IDENTIFY NEW REVENUE STREAMS

There's more than one way to successfully generate revenue, and now is the time to get started exploring options.



Continued on Page 3 ...