February 2023

TechSage Tech Talk

Insider Tips to Make Your Business Run Faster, Easier and More Profitable

INSIDE THIS ISSUE:

Add An Extra Layer Of Cyber Security Protection By Utilizing Cyber Insurance Page 1

Are You Enforcing Security Training For Your Team? Page 2

Shiny New Gadget of the Month Page 3

Have You Had Data Exposed In A Recent Data Breach Page 3

4 Ways To Answers Questions Like A CEO Page 3

Mobile Malware Has Increased 500% - What Should you Do? Page 4

We love technology and We love helping people.

Give me a call to find out whether we can help you better secure your data and get more out of technology.

-John Hill
Founder CEO

Add An Extra Layer Of Cyber Security Protection By Utilizing Cyber Insurance

Establishing effective and efficient cyber security policies is one of the most important aspects of protecting your business. We often discuss why cyber security is so important and the different cyber security practices your business can implement.

We also mention how advanced cyber-threats and cyber-attacks have become as hackers improve their tactics and technology. For this reason, you may wonder if there's anything that will cover your business if it falls victim to a cyber-attack even though you have strong cybersecurity practices in place.

Thankfully, cyber insurance is available to business owners who have proven they take cyber security seriously.

Cyber insurance (sometimes referred to as cyber liability insurance) is the coverage an organization can acquire to protect against losses incurred by a data breach or other malicious security incidents. Cyber insurance policies have grown exponentially in popularity over the past few decades as cybercriminals have become more cunning. Because of this, cyber insurance prices have also risen, so you may be curious whether cyber insurance is something your business absolutely needs.

Cyber insurance policies differ from provider to provider, but most will include the following coverages:

Customer And Employee Outreach
If your business is the victim of a cyber-attack and precious information is stolen, who are some of the first people you need to contact? Your customers and employees, of course. They need to be aware that a cyber-attack occurred, and their information may have been compromised. Depending on your industry and location, there may be a legal obligation to inform. If you have a large customer base, notifying them of a cyber security breach can be expensive. Cyber insurance will help cover those costs.

Recovering Stolen Data
It can be costly to hire a data recovery professional to recover stolen customer or business information, but it is necessary after suffering a cyber-attack. Most cyber insurance policies will pay for a professional's help.

Software And Hardware Repair/ Replacement
Cybercriminals can wreak havoc on

Continued on pg.2

Continued from pg.1

your software and hardware. If they damage or corrupt your computers, network or programs, your cyber insurance policy will help cover the cost of repair or replacement.

Some insurance policies will also cover any financial loss due to business interruption caused by a cyber-attack and ransomware demands. Cyber insurance will not cover your system upgrades, estimated future financial losses due to a breach or decreased valuation of your business caused by a cyber-attack. It's vital you know exactly what is covered by your policy before beginning coverage.

Starting a new cyber insurance policy is easier said than done. Since cyber insurance has grown in popularity, most providers have become more selective about who they cover, meaning you have to meet some criteria to qualify for a policy. The most essential thing any cyber insurance provider will look at will be the strength of your current network security and cyber security practices. Ensure you utilize multifactor authentication throughout your entire business and hold training sessions annually with your team. Purchase a firewall and do whatever else you can to improve your security.

> **"Cyber insurance can help further protect your business if you become the victim of a cyber-attack."**

If you don't, the rates for your policy will be astronomical, if you can even get one at all.

Suppose your business is within an industry that requires a certain level of cyber security compliance. In that case, you should be meeting your requirements or else you won't qualify for a cyber insurance policy. This shouldn't be an issue for your business since you must be compliant regardless of your interest in cyber insurance. Just make sure you look into your compliance requirements before applying for a cyber insurance policy to ensure you don't get denied coverage.

If you work with third-party vendors, you must do your due diligence and ensure they meet their cyber security requirements. Doing thorough research on the parties you interact with will help you get more affordable cyber insurance rates. Additionally, it would be best if you had an incident response plan in place. The insurance provider needs to know you're prepared to help your customers and your business if disaster strikes.

Cyber insurance can help further protect your business if you become the victim of a cyber-attack. In today's society, where every business and their customers' information is a target for cybercriminals, make sure you're as secure as possible. Build a strong cyber security plan and apply for cyber insurance to get maximum protection.

Cartoon Of The Month

Shiny New Gadget Of The Month:
NEBULA CAPSULE 3 LASER

Portable projectors are no longer a thing of science fiction or a concept of a distant future.

The Nebula Capsule 3 is around the size of your average tall canned beverage and can project an image with stunning 1080p resolution.

With its 52Wh battery, you can watch movies for up to 2.5 hours on a single charge (or plug in for longer use). And with a fully fledged Android 11.0 OS you have all of your favorite streaming service loaded right on the device!

HAVE YOU HAD DATA EXPOSED IN A RECENT DATA BREACH

There's a reason that browsers like Edge have added breached password notifications. Data breaches are an unfortunate part of life. And can have costly consequences for individuals. Hackers can steal identities and compromise bank accounts, just to name a couple.

Cybercriminals breach about 4,800 websites every month with form jacking code. It has become all too common to hear of a large hotel chain or social media company exposing customer data.

- **Microsoft Customer Data Breach**
- **5 Million Records Exposed in a Student Loan Breach**
- **U-Haul Data Breach of 2.2 Million Individuals' Data**
- **Neopets Breach May Have Compromised 69 Million Accounts**
- **One Employee Computer Causes a Marriott Breach**
- **Shield Health Care Group Exposes Up to 2 Million Records**

4 Ways To Answers Questions Like A CEO

I've had the privilege of posing questions to over 1,000 business leaders. So, I've been on the receiving end of many excellent answers from some of the most respected CEOs on the planet. On the other side of that, I've also heard responses from less skilled managers.

I've learned a lot through this process and would like to share some of that knowledge with you. Here are four ways to answer questions like a CEO.

1. **Answer a yes or no question with a 'Yes' or 'No' before providing details.**

   Does John Thomas work at Google?

   Bad Answer: "John Thomas? Oh, I knew him back at the University of Michigan. He and I were in the same engineering lab. This one time …"

   Great Answer: "Yes. John Thomas works at Google now. We went to college together, and we are friends on Facebook."

2. **Answer a number question with a number answer before providing details.**

   How much did your sales decline during the last recession in '08?

   Bad Answer: "The Great Recession was a really hard time for us. It felt like we ran a marathon in quicksand. No matter what we did, customers just stopped buying …"

   Great Answer: "Twenty percent. Our sales declined by 20%. Fortunately, our team's compensation was largely variable, so we all just made a bit less income during that period and were able to avoid any layoffs."

3. **Answer from the other person's point of view.**

   Why do you want me to invest in your ice cream stores?

   Bad Answer: "Because we need the capital to grow. And we need a way for some of our cousins to cash out of the business. This store has been in our family for 50 years."

   Great Answer: "Because a 10% return on invested capital is what you say you want. And that is what we have delivered reliably on a per-store basis for over 50 years."

4. **Share just enough information to prove your point but not more.**

   Why should we buy from your company?

   Bad Answer: "I could give you a million reasons to buy from our company. For starters, here is our 150-page brochure. And here is a 25-page PowerPoint slide deck in 8-point font. And here's …"

   Great Answer: "I think you should buy from us for three reasons: Gartner Group rated us #1 in the three areas that are most important to you: ease of implementation, security and customizability for multiple languages. In addition to this, we know this space better than anybody. Our team published the #1 book on Amazon about this topic. And, lastly, we offer a 100% money-back guarantee, so the burden of risk will be on me, not you."

Using these tactics will give you a much better chance of being hired at your dream job or persuading investors.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

MOBILE MALWARE HAS INCREASED 500% - WHAT SHOULD YOU DO?

Cybersecurity researchers uncovered an alarming mobile statistic. During the first few months of 2022, mobile malware attacks surged by 500%.

For years, mobile phones have become more powerful. They now do many of the same functions as a computer. Yet, people tend to secure their computers better than they do their smartphones. This is a behavior that needs to change. Over 60% of digital fraud now occurs through mobile devices. That makes them highly risky if proper safeguards aren't followed.

Use Mobile Anti-malware

Yes, your mobile phone needs antivirus/anti-malware too! Malware can and does infect smartphones and tablets. Ensure that you have a reliable mobile anti-malware app installed.

Don't Download Apps from Unknown Sources

Only download mobile apps from trusted sources. Do not download outside a main app store. Trusted app stores include places like:

- Apple App Store
- Google Play
- The Microsoft Store
- Amazon Appstore

Don't Assume Email is Safe

Many people prefer checking email on their phone rather than PC because it's so handy. But they have a false sense of security about the safety of emails when viewed on a mobile device. It's difficult to hover over a link without clicking when on a smartphone. If you see something questionable and want to check the link, open the email on your PC where you can do that.

Beware of SMS Phishing (aka "Smishing")

In March of 2022, text spam outpaced robocalls. Unwanted text messages rose by 30%, ten percent higher than robocalls. Many of those spam texts are smishing. Be on the lookout for text messages that don't quite make sense. For example, getting a shipping notification when you haven't ordered anything.

Remove Old Apps You No Longer Use

Go through your device and remove old applications that you are no longer using. There is no reason to keep them around, potentially leaving your device at risk.

Keep Your Device Updated

Speaking of updates, you also need to keep your device's operating system updated. Are you using the current version of Android or iOS? Not installing updates can mean your phone has vulnerabilities. These vulnerabilities allow hackers to breach your data.

Use a VPN When on Public Wi-Fi

Public Wi-Fi is dangerous. Most people understand that, but many connect to it out of necessity. Reduce your risk by using a VPN app.

Mobile Security Solutions to Prevent a Data Breach

Don't wait until your phone is infected with malware to secure it properly. It's only a matter of time before you are the next victim.

Education is the most powerful weapon which you can use to change the world.

—Nelson Mandela