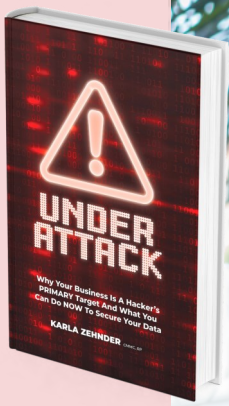
TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON CONSULTING & SOLUTIONS

What's New

UNDER ATTACK
By Karla Zehnder



We are excited to announce a new book release, Under Attack written by our CEO Karla Zehnder.

This book will be jam-packed with valuable information, tips and strategies on how to PROTECT your business from cybercrime, viruses, malware attacks, hackers, downtime, disgruntled employees, and a number of other online threats that can shut down your business or cause major interruption.

SEE INSIDE FOR MORE DETAILS

September 2022

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

It's Time For A Refresh!

4 Cyber Security Trainings To Do With All Employees

Students are returning to the classroom now that back-to-school season is officially underway. During the first few weeks, teachers will be reteaching their students the topics they learned in the previous school year to help them regain knowledge they may have forgotten during summer break. But students aren't the only ones in need of a refresher every year. Your employees also need to be refreshed on company policies, values and, most importantly, cyber security practices.

Did you know that human error accounts for 95% of all successful cyber-attacks? When a cybercriminal is planning an attack, they look for weak points within a company's cyber security plan. The easiest spot for hackers to exploit is a company's employees. New cyberthreats are created on a consistent basis, and it's important that your employees know what to do when they encounter a potential threat. If your employees are not routinely participating in cyber security trainings, your business could be at risk, regardless of size.

Every single one of your employees should be familiar with your cyber security practices. When they're hired on, they should go through an initial training that lays out all of your practices, and they should also participate in refresher trainings throughout the year to ensure that the entire team is on the same page with cyber security. At the very least, you should host at least one security training annually. If you've never put together a cyber security training, you may be wondering what topics you need to cover with your team. Below, you will find four of the most important topics to cover.

Responsibility For Company Data

This is your opportunity to explain to

Continued on pg.2

Continued from pg.1

your employees why cyber security is so important. They need to understand why cybercriminals are interested in your company's data and what they could potentially do with it. Everyone on your team has a legal and regulatory obligation to protect the privacy of your company's information. When discussing this topic with your team, it's imperative that they know the ramifications of falling victim to a cyber security threat.

> **"Human error accounts for 95% of all successful cyber-attacks."**

Internet Usage

Does your company have restrictions on what websites your employees can use while at work? If not, that's something you should look into. Every device that's used by your employees should have safe browsing software downloaded onto it to prevent them from stumbling upon dangerous sites that could put your company's data at risk. Your employees should know what sites are acceptable to use and that they should not be accessing their personal accounts while connected to your company's network. They should never click on links that are sent from an anonymous source or are found on an unapproved website.

E-mail

If your employees utilize e-mail while at work, it's important that they know which e-mails are safe to open. Employees should not respond to e-mails that are from people they aren't familiar with, as that could be a cybercriminal attempting to gain access to your company's data. Employees should only accept and open e-mails that they are expecting or that come from a familiar e-mail address.

Protecting Their Computers

If your employees have their own personal computers, they should be doing everything in their power to keep them protected. Whenever they walk away from their computer, they should make sure it's locked; they should also never leave their computer in an unsecure location. Also, ensure that your employees are backing up their data routinely and have downloaded the necessary antivirus software.

It's of the utmost importance that your team has been fully trained in your cyber security practices. If they haven't, they could open your business up to all sorts of cyber-attacks that will damage your company's reputation from a customer perspective. Your business will also no longer be compliant, and insurance companies may not cover your claims if your team is not participating in regular training.

Ensuring that your team is aware of your cyber security practices and actively taking steps to strengthen your cyber security is the best way to stay compliant and prevent cyber-attacks. If your team is not regularly going through cyber security training, you need to start. It will offer more protection to your business, which will make your customers more comfortable doing business with your company.

Disaster Data Recovery:
Are You Prepared?

Most businesses have now gone digital, taking their processes online and storing data in the cloud. While speedier transactions and greater portability make this technique very convenient, it also poses some risks. One of these is the risk of digital disasters and possible security breaches from all directions. In other words, if you aren't vigilant, all of your company's data can be stolen or encrypted.

Unforeseen Disasters and Breaches in 2021

In recent years, there have been numerous disasters that have affected global companies in different industries. Most of the attacks in 2021 came in the form of ransomware that took advantage of human gullibility.

The electronics company Acer took a hard blow in cyber-attacks in 2021. Overall, they ended up dealing with a $50 million ransom demand that a notorious hacking entity called ReEvil supposedly asked for in exchange for the return of a massive amount of stolen digital data.

In April of last year, Facebook suffered a security breach that exposed the personal information of over 530 million users. Screen scraping is a technique used by hackers to get information from websites. It's how they were able to access the data files of almost 92% of LinkedIn members and obtain personal details like emails or phone numbers!

Because of the lockdowns and work-from-home setups, previously protected information became exposed in the digital world. Luckily, most companies had reliable security policies that protected data coming in and out of their office networks. However, with many individuals working remotely and using devices, it is difficult for a corporation to keep control over their security network, necessitating an upgrade.

The Importance of Proper Preparation and Safeguarding Your Business

Business owners often make the mistake of believing that something like this will never happen to their company. They like to believe that because they are a tiny firm, no hacker would be interested in attempting to compromise them. As a result, many don't even bother to take precautionary measures to protect their small or medium-sized businesses from potential threats.

Unfortunately, small and medium-sized businesses are easy to crack and are typical targets of these hackers. Many companies lack the appropriate infrastructure and security tools to protect themselves from cyberattacks. To keep from being a victim, you must partner with a managed services provider that can provide you with an ironclad disaster data recovery plan.

Creating a Good Disaster Recovery Plan

Disaster data recovery is a serious matter that should not be taken lightly. The process of developing this plan entails a great deal of deliberation and decision-making.

Begin by defining a sensible recovery time objective (RTO). This process is the amount of time you expect to be fully back on track after disaster strikes. The shorter the RTO, the more expensive the disaster data recovery will be, so you need to consider this.

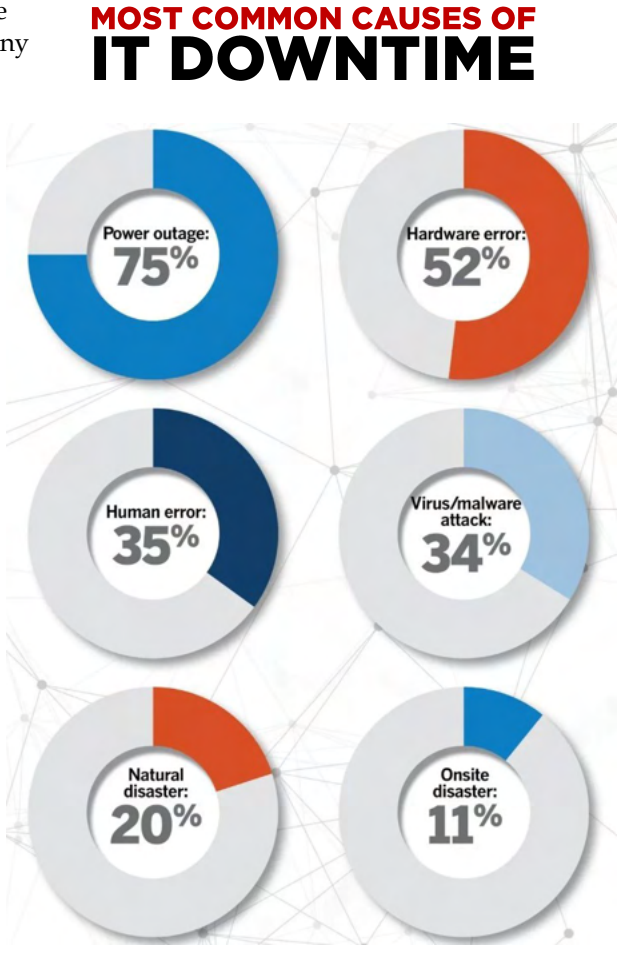
Also, make sure to clearly outline the duties and responsibilities of each individual employee in your organization. In addition, establish a clear communication plan as well as security protocols.

Of course, the most crucial parts of disaster data recovery are having offsite data backup and installing dependable and updated anti-spyware tools on all the devices used for business procedures. You should also test your disaster recovery plan with your staff. That is the only way to find out if it works.

Hire a Professional MSP for Disaster Recovery

As you can imagine, disaster recovery is a complex matter. If you want to know that your plan can protect you, the best option is to have a fully managed disaster data recovery solution from a reliable MSP.

Ensure the safety of your company now before it is too late! Contact us today, and we will show you how.



These Marketing Trends Didn't Go Out Of Style

When people think about trends, they often imagine what's in style at that current moment. We like to imagine that trends come and go, but the opposite is sometimes true. In fact, the greatest trends become a part of our culture. At one time, people thought cellphones, texting and computers were just a phase, but decades later, they're still here because they made our lives better! Trends in marketing are the same.

Sometimes a fresh marketing strategy will pop up, but if it works, it will become a mainstay.

As you continue to plan your marketing strategy for the next few months and the upcoming year, you can look at previous statistics to ensure your methods are successful. Below, you will find three marketing strategies that have proven successful in the past. If these strategies are properly utilized by your company, you will quickly see results.

Using Influencers

People love to use their smartphones and social media. During the pandemic, many businesses started to advertise on Instagram and TikTok through the use of social media influencers. A TopRank Marketing survey found most B2B marketers believe this strategy changes minds, improves the brand experience and yields better campaign results.

Advertising On Podcasts

There are podcasts available that discuss every topic imaginable, and over 30% of Americans listen to a podcast on a monthly basis. That percentage rises when you look at younger demographics. Advertising on podcasts is a great way to reach a younger audience.

Leveraging AI

The importance of artificial intelligence (AI) for B2B marketing became crystal clear recently, when a Salesforce study reported that 80% of business buyers expect the companies they reach out to will talk to them "in real time," regardless of the hour. This statistic highlights how important chatbots and other AI solutions are for customer conversion.

If you've seen success with certain marketing trends in the past, you don't have to get rid of them when you develop a new marketing strategy.

Cartoon Of The Month

"I just feel fortunate to live in a world with so much disinformation at my fingertips."