1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

What Is Cyber, Crime, And Social Engineering Insurance ……..Page 1

FREE: Dark Web Scan ……Page 2

Security Corner: Avoid DDoS Attacks In 2022 ……..Page 3

Why Having A Continuity Plan Is A Sign Of Great Leadership ……Page 3

Reduce Workplace Stress By Using Technology ……Page 4

April 2022

Kim Nielsen
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

What Is Cyber, Crime And Social Engineering Insurance?

Most people have heard of cyber insurance. News of cyber breaches grace the headlines almost weekly these days. But are you really covered for all types of thefts committed using the latest technology? The answer is probably not, especially if you aren't purchasing crime insurance. Let's take a look at what you're covered for under a cyber and crime policy.

Cyber Insurance for Theft of Data
Cyber gets plenty of shine as one of the hottest insurance products on the market. Cybercrime events lead the headlines frequently. Many states are enacting special response regulatory guidelines. Due to this activity, insurance carriers responded by creating one of the broadest products on the market. While every insurance policy is different, what does it actually cover? A comprehensive cyber program should cover your directs costs and liability to a 3rd party after a cyber event. Some of these direct costs can include:

- Event management costs which include costs for forensics services, notification expenses. Includes call center costs, legal services, identity monitoring and engaging a PR firm as well.
- Costs to recover and restore lost data corrupted or destroyed after a computer attack.
- Cyber extortion costs including the expenses for consultants and the demand.

Business Interruption reimbursement for loss of income and extra expenses to get up and back running after a cyber event that causes your system to fail or the failure of computer system maintained by a vendor. Despite the broad language in cyber policies, gaps in coverage still exist. Next we'll take a look at crime insurance.

Crime Insurance for Theft of Money
With cyber getting all the shine, many overlook the need for crime insurance. Crime insurance has evolved to cover

Continued on pg.2

Continued from pg.1

much more than employee theft as bad actors have become more sophisticated. Crime insurance is fundamentally designed to cover the theft of money. It covers the more traditional methods of theft including robbery, burglary, and forgery. But honestly, criminals are now committing these crimes from the comfort of their own home. Traditional crime insurance continues to expand to cover new types of theft as technology rapidly changes. Policies now cover fraudulent instructions sent electronically or physically (telephone, fax, etc.) instructing banks to transfer your company funds to another account.

Crime Insurance, Social Engineering and Using Stolen Information to Steal Money

Nowadays, bad actors are passing the bank and giving fraudulent transfer instructions directly to employees. Most people believe their employees would never fall for such a scam. These schemes are more common than you would think and often very successful! Essentially, criminals are using a virus, phishing or other traditional hacking methods to steal information. The stolen information will allow them to pretend to be an authorized employee to instruct others to make transfers.

This scheme has many names including social engineering, cyber crime, computer crime, spear phishing etc. Basically, social engineering is the place where cyber and crime meet. While coverage for cyber crime is available under both crime and cyber policies by request, most underwriters agree that social engineering is just a new method for theft of money. Crime insurance policies specifically cover only the theft of money. Some examples of the type of scams potentially covered under the social engineering coverage are:

- Bad actor hacks into the CEO's email and sends an urgent message to the approved person to make transfers requesting funds transferred to an account for a top secret deal.
- Cybercriminal collects publicly available information to impersonate an executive and instructs an individual to make a transfer of funds.
- Employee inserts an infected storage device into a local network that allows the criminal enough access to enable the transfer of funds.
-
- Employee responds to a seemingly legitimate email and voluntarily provides enough sensitive information that allows someone to pose as that person to initiate a funds transfer directly or through another employee also known as phishing.

Takeaways

In this era, every company has some sort of cyber and crime exposure. Cyber and crime insurance experts agree, it's not if it's when. Make sure your insurance program is broad enough to cover any type of cyber attack regardless of the method or what was stolen. The best way to do that is purchase both a cyber and crime with social engineering policy.

Every company has some sort of cyber crime exposure

Do You Safeguard Your Business And Your Customers' Private Information BETTER THAN Equifax and Target Did?

If the answer is "NO" – and let's be honest, the answer *is* no – you are leaving yourself and your company open to massive liability, ***millions*** in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s),

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits, and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers. *Reserve your exclusive Dark Web Scan* ***now****!*

Get your free Dark Web Scan TODAY at:
https://www.cti-mi.com/dark-web-scan-422

Security Corner

Avoid DDoS Attacks in 2022

It's one of the most frustrating interruptions to a workday when your website or service crashes right at peak traffic times. This can be as simply solved as restarting its power source, or as sinister as a denial-of-service attack (DDoS) that's targeting your business.

What is a DDoS Attack?

Distributed denial-of-service threats occur when bad actors connect machines from many remote locations, and force them to overload your servers and crash the site.

Why Do DDoS Attacks Happen?

You may be wondering what cybercriminals have to gain from halting legitimate traffic to your website. They might use this distraction to steal private files from the organization, or it could be purely out of retaliation that they try to cause financial or reputational damage.

DNS Monitoring

Domain name systems, or DNS, change website domains into IP addresses that the computer can understand and redirect to. DNS monitoring assesses the connection between visitors and your website to guarantee that these processes go uninterrupted.

With rates of distributed denial-of-service attacks still rising as we progress into the year, proactive response plans are your best defense.

For more information on DDoS attacks and how to prevent them, call us at 248-362-3800 or visit: https://bit.ly/3x2k9wL

Why Having a Continuity Plan Is a Sign of Great Leadership

Your business faces all sorts of threats that can disrupt your operations. A comprehensive continuity plan can help address them. Carrying on with business as usual is easy when nothing out of the ordinary is happening. But the fact is, crises can strike anytime.

And when it happens, you need to be ready to pivot your operations quickly, safely, and efficiently. That's where a well-thought-out business continuity plan comes into play. It prepares you for the worst, such as market nosedives and governments shutting down entire countries. And in these cases, your plan allows you to embrace remote work, enabling you to keep functioning and servicing your clients. It also lets you support your team at home and make them feel comfortable through various predicaments.

It can safeguard against financial loss, lost productivity, and a damaged reputation. On top of that, it helps protect your employees from injuries or death in case of threats. The overall effect can be a reduced risk of losing your business and team members.

But what specific threats can you address with a continuity plan?

Threat #1. Natural Disasters Natural disasters are extreme geographic phenomena, including tornados, tsunamis, volcanic eruptions, wildfires, and earthquakes. They're tricky because they're hard to predict and can leave disastrous consequences within seconds.

Threat #2. Utility Outages Water shutoffs and loss of communication lines or power can hinder your daily operations. Without a continuity plan, the risk of asset damage and productivity loss is drastically higher.

Threat #3. Cybersecurity Cyberattacks are computer-based attacks on your technical assets. In the best-case scenario, your infrastructure will function less efficiently until you resolve the issue. But in the worst-case scenario, you could lose access to all business data.

Create the Best Continuity Plan
Developing a foolproof continuity plan requires a systematic approach involving:

#1. Identifying Goals Business continuity doesn't just comprise your IT systems. It encompasses all essential business functions, like public relations, human resources, and operations.

#2. Setup Emergency Preparedness Group Choose several cross-functional managers and anyone else who can contribute to the plan, such as your IT service provider.

#3. Business Impact Analysis and Risk Assessment Identify, research, and analyze your potential threats thoroughly.

#4. Focusing on Customer Service Your clients need empathy and transparency during crises.

#5. Addressing Business Function Your plan should incorporate critical business functions. These include business risk, impact on customers and employees, emergency policy creating, community partners or external organizations, and financial resources during disasters.

#6. Staff Training and Plan Updates Present your continuity plan to stakeholders and promote a proactive approach through trial runs to verify the plan works.

Don't Let Crises Cripple Your Business
Disasters can be the ultimate test of your leadership abilities. That's why instead of leaving your company to chance, create an in-depth business continuity plan before emergencies arise. Make sure everyone is on the same page, and you'll be able to come out stronger after any predicament. For more information or assistance with developing a continuity plan, call us at 248-362-3800.

Reduce Workplace Stress By Using Technology

Many business owners focus on reducing work-related stress to keep their employees active and healthy. This way, they can focus more on their work instead of taking leave. Your employees should feel motivated while they are in the workspace. This way, they can evaluate and organize their life in a better way to ensure optimal work and life balance.

Why Should You Reduce Stress? You should reduce workspace stress for numerous reasons. To know the importance of reducing stress, you must understand how it affects your employees' physical and mental health, impact business activities, and hinder any progress towards long-term goals.

Reduce Stress with Technology The main reason for workspace stress is a lack of productivity and focus. However, you can utilize technology for good, thereby reducing stressful work routines. Numerous applications are available to help your employees focus and manage their routine. Here, we will discuss some of those tools:

Project Management Managing projects without any tools is a hectic task. Planning, prioritizing, and tracking tasks will take up a lot of your time. However, you can rely on different tools to perform these activities. Integrate those tools, so your employees don't feel burdened. You can choose between popular tools such as Asana and Trello.

"I always play the GPS throught the backseat speakers. That's where I'm used to receiving instructions."

Time Management When your employees are unable to focus and perform tasks due to stress, they can't practice effective time management. Eventually, this will add to their stress and pressure. Tools such as Pomodoro are an amazing option to manage time in your workplace. When your employees meet deadlines, they can focus on other tasks or relax.

Collaboration Other time-consuming activities involve collaborating and communicating with colleagues. You can streamline internal communication by integrating tools such as Slack, Google Drive, and Basecamp. These tools will not only help your employees communicate with each other, but they can also share and receive files and track their tasks. Furthermore, these tools will keep your tasks and conversations organized for quick and easy future reference.

Stress Relief Apps You can introduce various stress reducing applications among employees. For instance, applications that reduce anxiety will keep your employees calm and happy. You can share these applications that make it mandatory to relax for five minutes after working for an hour. Applications such as Mindwell and The Breathing App are popular for reducing stress.

Increasing workload and giving your employees a tough time will have a negative effect on your business. With excessive stress, your tasks will become counterproductive, and employees will lose their focus. If you want to improve employees' productivity, start by reducing workplace stress.