CSU Connection
Serving our community for over 30 years
February 2023

Cybersecurity Insurance is Changing

Cyber liability Insurance has become an ever-evolving market. It is used to cover everything from data processing errors and online scams to malware infections. The increase in online danger and rising costs of a breach have led to drastic changes in cyber insurance. It's important to review your cyber insurance policy at leastonce a year and ensure you know what is covered and excluded.

Here are a few areas to check "Does my policy cover":

- Recovering compromised data – via ransomware such as Cryptolocker
- Repairing computer systems in the case of ransomware
- Costs associated with notifying customers about a data breach – mailouts, credit monitoring, etc.
- IT forensics costs to investigate a breach
- Legal expenses concerning client lawsuits over the breach
- Expenses for the downtime while forensics is researching – employee costs, lost revenue, etc.
- Ransomware payments – hopefully, you're using our backup services, so you won't have to pay the ransom ~ but if you're not, will they pay the bad guys for your data?

This list isn't exhaustive; it's the baseline of questions to which you should know the answer regarding your cyber insurance policy.

And you may want to ask, "If I have an incident, how long do I have to wait for you to "investigate" before I can restore my backup or do whatever it takes to get back to work?" If your agent says they can't provide an exact time frame, ask them to give you a ball park estimate based on other claims they've seen processed. Someone there has that answer.

Here are a few things to keep in mind this year regarding Cyber Insurance:

1. Demand is Going Up

The average cost of a data breach is currently $4.35million (global average). In the U.S., it's more than double that, at $9.44 million. As these costs continue to balloon, so does the demand for cybersecurity insurance. Companies of all types realize that cyber insurance is critical and as vital as their business liability insurance.

2. Premiums are Increasing

With the increase in cyberattacks has come an increase in insurance payouts. Insurance companies are increasing premiums to keep up. In 2021, cyber insurance premiums rose by a staggering 74%.

Insurance carriers aren't willing to lose money on cybersecurity policies.

All you need is love. But a little chocolate now and then doesn't hurt.
-Charles M. Shulz

Our Mission

is to deliver outstanding IT support to your business in order to improve uptime, productivity. and profitability.

You take care of running your business, we'll take care of your technology.

cont. on pg 2

3. Certain Coverages are Being Dropped

Certain types of coverage are getting more difficult to find. For example, some insurance carriers are dropping coverage for "nation-state" attacks. These are attacks that come from a government, and many governments have ties to known hacking groups. So, a ransomware attack that hits consumers and businesses can very well be in this category.

In 2021, 21% of nation-state attacks targeted consumers, and 79% targeted enterprises. You may want to ask your agent what information they use to classify cybercriminals as "nation-state" actors. Another type of attack payout that is being dropped from some policies is ransomware. Insurance carriers are tired of unsecured clients relying on them to pay the ransom. So many are excluding ransomware payouts from policies, which puts a bigger burden on businesses.

4. It's Getting Harder to Qualify

Unlike every other insurance, just because you want cybersecurity insurance doesn't mean you'll qualify for it, and if you do, the premium may be outrageous. Insurance carriers aren't willing to take chances, especially on companies with poor cyber hygiene (lack of security protocols).

Here are some of the factors that insurance carriers are looking at:

- Network security
- Use of things like multi-factor authentication or biometrics
- BYOD (how many employees are using their own devices) and device security policies
- Advanced threat protection
- Automated security processes
- Backup and recovery strategy
- Anti-phishing tactics
- Employee security training
- Physical security

With the new year just starting, now would be a great time to review your current cyber insurance policy and how your business aligns with your coverage.

Have You Been Exposed in a Recent Data Breach?

There's a reason that browsers like Edge have added breached password notifcations. 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*

Gadget of the Month:

Petcube Bites 2
Pet Camera with Treat Dispenser

With this ultimate assistant for busy fur parents, you can:

- Fling treats short, medium, or long-distance for play or reward.
- Have peace of mind your pet is safe with full 1080p HD live streaming video, 160° ultra-wide-angle lens, 4x digital zoom, and night vision.
- Say hello or tell them to stop if you catch them at mischief with 2-way audio connected right to your smartphone.
- Get notified of major disturbances with smart alerts, triggered by sound and/or motion at home.

Get yours today on Amazon!

February is Bonnie's Birthday Month!

Henry Ford once said: *"Anyone who stops learning is old, whether at 20 or 80. Anyone who keeps learning is young."*

Celebrating her 79th, we celebrate our highly valued colleague and friend who loves learning and continues to grow and contribute to CSU with her vibrant spirit!

Happy Birthday Bonnie! We appreciate you!

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 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

Do not 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 User

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. Areyou using the current version ofAndroid or iOS? Not installing updates can mean your phone has vulnerabilties. 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.

What's new at CSU?

Roses Are Red
Violets Are Blue
Hackers Are Lurking
Don't Let Them
Get You!

Introducing...
Monthly Coffee Break Webinars

When: *At your leisure*

How long: *<10 minutes*

Where: *Our website:*
www.csuinc.com/coffee

Free of cost!

Welcome Emily!

We are thrilled to have Emily join our CSU family. She is energetic, bubbly, happy, and fun!

Join us for *Phishing 101*: With so many incoming emails on all your devices, we'll show you the most common phishing methods and what to look out for.

Valentine's Day: the "Holiday of Love"

One legend contends that St. Valentine was a priest who served during the third century in Rome. When Emperor Claudius II decided that single men made better soldiers than those with wives and families, he outlawed marriage for young men.

Valentine, realizing the injustice of the decree, defied Claudius and continued to perform marriages for young lovers in secret. When Valentine's actions were discovered, Claudius ordered that he be put to death; making Valentine a martyr for love.

Letters to Juliet

Every year, thousands of romantics send letters adressed to Verona, Italy to "Juliet," from the timeless romantic Shakespearean tragedy, "Romeo and Juliet". They are read by a team of volunteers called the Juliet Club.

On Valentine's Day, the club awards the "Cara Giulietta" ("Dear Juliet") prize to the author of the most touching love letter.

Get connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

703.968.2600