CSU Connection
Serving our community for over 30 years
April 2023

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.

"Start where you are, with what you have.
Make something of it and never be satisfied."
— George Washington Carver

in this issue...

Happy Spring!

Data Backup is Not Enough! You Also Need Data Protection.

The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. There are about 140,000 hard drive crashes in the US weekly. Every five years, 20% of SMBs suffer data loss due to a major disaster. This has helped to drive a robust cloud backup market that continues to grow. But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

What does this mean?
It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats.

Some of the modern threats to data backups include:

Data Center Outage:
The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.

Sleeper Ransomware:
This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore.

Supply Chain Attacks:
Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.

Misconfiguration:
Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

What to Look for in a Data Protection Backup System
Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

Ransomware Prevention
Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

It's important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

Continuous Data Protection
Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

cont. on pg 2

Threat Identification
Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop sleeper ransomware and similar malware from infecting all backups.

Zero-Trust Tactics
Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safelisting.

Top 5 Ways to Protect Your Business from Ransomware

There are concrete steps you can take to make it difficult for hackers to sneak their way into your computers and network.

How bad is the ransomware problem?
According to the Verizon 2021 Data Breach Investigation Report ransomware has more than doubled year-over-year. And attackers are targeting companies of all sizes – no one is too small.

There are ***4 kinds of ransomware***:

1.Encryption – the most common type of ransomware, which encrypts all of your data and makes it impossible to unlock without a decryption key.
2. Lockers - restrict the use of your computer, making it impossible to work or use essential functions until the ransom is paid. This form of ransomware is not used as much today.
3. Scareware - attempts to scare users into buying unnecessary software, giving control of your computer to the hackers, or having your money stolen.
4. Dovware / Leakware - threatens to leak personal or company information unless the ransom is paid.

These are not the only ways to get a ransomware infection running rampant in your network, but they are the most common.
You'll know when you've been hit by ransomware: The attack typically starts at one workstation (the geek speak term is an "endpoint").
Once implanted, the ransomware runs silently in the background. It will often search your network for other targets to encrypt, including file servers, other workstations, and backups. The more files it can encrypt, the more likely you will pay the ransom, regardless of the price demanded.
Once it's encrypted all the files it can, a message will pop up on your monitor telling you that your files are locked and demand that you pay a ransom, typically in some cryptocurrency like Bitcoin.
The hackers also give you a deadline to pay, or your files will be permanently locked. Some of these attacks are so sophisticated that the attackers have a support team that you can call or email for help on making the cryptocurrency payment.
If you get the ransomware message on your computer, **it's essential to stay calm and not panic**. The hackers want you to panic so you'll make rash decisions.

These tips can help prevent you from being a ransomware victim. These **next five protections** are the minimums that every business should have to protect itself in today's threat landscape, no matter their size.

1. Protect your email: Whether it's downloading attachments, clicking on links that go to infected websites, or tricking users into giving up their usernames and passwords – email is the main door used to get in. Ensure you're using a spam filter/email protection that provides advanced multilayered protection and includes AI-enabled learning and real-time analytics. If you're using Microsoft O365 or Gmail, this would be in addition to the standard services.

2. Install Antivirus Software & a Firewall: Please do not use the "free" versions of antivirus software. They are free because they don't keep up with all the latest threats. Antivirus software is essential in defending against ransomware as it can scan, detect, and respond (quarantine/delete) to cyber threats.

You'll also need a firewall since antivirus software only works at the internal level and can only detect the attack once it is in the system. A firewall is often the first line of defense against any incoming external attacks. It can protect against both software and hardware-based attacks. A firewall is essential even if you're a small business or work from home.

3. Backup Your Data: Data is the engine that drives your business; without it, your business doesn't run. Besides not getting it at all, the easiest way to recover from ransomware is to have all your systems and data backed up with a current working copy stored OFF the network. This ensures that the hackers can't delete or encrypt your backups!

4. Keep Systems & Software Patched & Updated: Keep your operating system, web browser, antivirus, and any other software you use updated to the latest version. Malware, viruses, and ransomware are constantly evolving with new variants that can bypass your old security features.

5. Security Awareness Training: Humans need to be at the heart of any cybersecurity strategy. According to the 2022 Verizon Data Breach Investigations Report, 82% of data breaches involved human interaction.

Download our free printable with these reminders to hang up in your office for you and your team!

www.csuinc.com/coffee

Your security training should include spotting and reporting suspicious emails, staying safe while surfing the web and social media, and securing personal devices and home networks if they work from home.

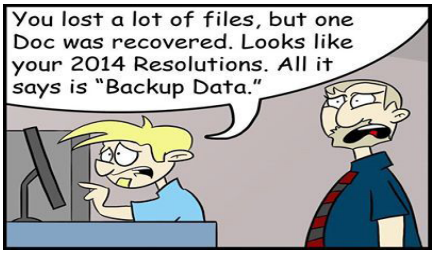
Security training for employees should be at minimum once a year – twice a year is better, and quarterly is best, so they stay current with the latest trends and security is top of mind.

Cyber Insurance is NOT on this list.
While you absolutely should have cyber insurance, you should NOT use insurance **alone** as a protection method. Too many businesses owners have said, "Yeah, I have insurance, so I don't have to worry about any other security protections," and have had their claims denied because they didn't have these basic protections in place.

According to Bloomberg Law, Ransomware claims have skyrocketed, accounting for nearly 75% of all claims filed. This explains why there are more questions and more "exclusions" with your insurance renewal each year. Most companies will see an increase of 25-30% in their premiums this year.

There are additional security layers and tools you can put in place to protect your business. Of course, despite all the security measures you may have in place, it's still possible to become a victim of ransomware. Being cautious goes a long way!

Every business should have a written ransomware security plan that includes what to do immediately after becoming infected or attacked, and who to contact with their names and phone numbers.



 cont. on pg 4

Gadget of the Month:

Chillwell Portable AC

Whether you're looking for a break from the sun or you prefer cooler temperatures while sleeping, ChillWell AC lets you control the conditions for improved work, leisure, and relaxation.

Take This Mini Air Cooler Anywhere!

It's portable and rechargeable
Travel from room to room or take it with you to the office for keeping cool wherever you go.

It's adjustable
The clean, modern design is well suited for any room. With 4 fan speeds and a variable vent for directing airflow, you can always optimize the cooling to your personal preference.

It's simple to use
With easy top-fill pouring, the ChillWell AC is designed to make your life easier.

Get yours today at chillwellshop.com

No re-fill tank to worry about, just pour the water directly into the unit for pleasant, humidified air.

Deciding When and How to Fire Clients

After firing eight clients for crabby behavior in one month, a hospital manager hung a poster in the lobby: **"We have zero tolerance for aggressive and abusive behavior."**

Fed up with uncalled-for entitlement, more managers are initiating "kindness policies" and notifying clients through mass emails, social media, and new client registration forms. Managers do not want their employees to fear for their safety or psychological well-being.

It is critical to any business to wisely and professionally handle difficult customers, and to especially know when it's time to draw the line and say goodbye and how to do it.

Continued on page 5

Defining which behaviors merit firing

Schedule a staff meeting to learn and practice conflict-resolution techniques so employees can react appropriately when situations arise. Professional in-the-moment responses may correct clients' bad behavior and set expectations for future interactions.

Business leaders should **define** reasons to fire clients, such as:

•Threatening or aggressive behavior and/or language
•Physical violence
•Discriminatory behavior
•Failure to honor business policies
•Refusing to pay for services and/or having outstanding balances
•Three or more no-shows for appointments and/or procedures

Correcting bad behavior on first instance

Let's say Mr. Friendly mutates into Mr. F-Bomb:

Explain the expected behavior and how it will result in a solution. Isolate the client by taking them into a private area such as a conference room, manager's office, or employee break room.

Say this: "So you may have my complete attention and we can find a solution together, let's step into the office."

Reducing his contact with an audience of other clients will de-escalate the situation and communicate your desire for an immediate resolution. Stand up so you and the angry client are on the same eye-level. If you are seated and the client is standing, he is in the dominate position. Walk and talk as you guide the client to a private area for further discussion.

To correct foul language, state benefits of respectful behavior.

Say this: If I hear that language again, I won't be able to help you with your issue/request. We need to find a better way to communicate so we can find a solution together."

The word "language: is neutral compared to "If you don't quit cursing," which may be perceived as confrontational and lead to more negative words. Use "we" to show collaboration rather than "you," which blames the client. . "Solution" communicates you want to resolve the issue. If bad language continues, ask the client to leave the building or explain you will hang up if it is a phone conversation.

Ejecting bullies

Don't be bullied by clients who should expletives. If unruly behavior continues, follow these steps to eject a bully from your establishment:

1. Assess the potential danger of the confrontation. Employees should seek support from a manager when a client becomes verbally abusive. The right words instruct the client to immediately correct the behavior.

Say this: "I understand that you are frustrated. We both need to be calm and work together to resolve this situation."

If a client appears to be under the influence of drugs or alcohol, offer to call a taxi. If the client is with others, ask a sober person to drive the offender home. If the impaired client insists on driving, get a description and/or photo of the car and license plate and call police with that information. You also may have security cameras that record the incident.

2. Explain why you are asking the client to leave. Abusive behavior will not be tolerated.

Say this:

•"While you have a right to voice your concerns, you do not have the right to be abusive to our staff."
•"As a manager, it's my responsibility to protect my team, other clients, and patients so I must ask you to leave the premise now."
•"If you don't leave our building voluntarily, I will call the police to protect my staff, clients, and patients."

3. Escort the client out of the building.

Use body language to reinforce your ejection of the client. Walk toward the exit and ask the client to follow you. Keep walking toward the door, even if the client doesn't initially follow you. Remain at the door. This firm body language communicates your request to leave is final and non-negotiable. Watch the client drive out of your parking lot. If the client sees you immediately leave the door, he or she may return inside.

4. Don't put your hands on the client.

Touching an irritated person could get a violent reaction.

Continued on page 6

5. Call the police if necessary.
Call the police if the client is threatening physical harm to you or others, breaking a law, or damaging business property. **Do not be timid.**

Look the client in the eye and **say this**: "Please leave the building immediately, or I will call the police." You are telling- not requesting- the client must leave now.

As clients will always challenge you, the best thing you can do is teach your team what to do **before** situations occur.
Like any good relationship, open communication and clear expectations will build trust and respect while preserving the reputation and integrity of your company.

Original article in April 2023 issue of Veterinary Practice News

Let's Celebrate!

CSU has some super special people to celebrate this month...

Happy Birthday to the one and only, Alyssa!

Did you know?
Alyssa can play 6 instruments and is an official music education major at George Mason University.
You go girl!!
She is fun, smart, determined, altogether awesome, and irreplaceable in the CSU family :) We love you Alyssa!

then- - - - *now*

Happy 25th Anniversary to the O.G. CSU employee, Mike!

Time flies when you're employed at CSU! Like any family member, Mike has grown alongside CSU since the beginning, ups and downs and all.

To express our gratitude for his loyalty and hard work over these last couple decades, CSU sent Mike and his wife to an all-inclusive resort in Jamaica.*(see pg. 7)*

You rock Mike!

Here's to 25 great years and more to come!

Thank you for going above and beyond taking the first step to meet our client's needs... We appreciate you so much!

Happy Birthday to our talented, patient, and seriously cool client care dispatcher- Heath!

Did you know? Heath won the Boston Music Award's Metal Artist of the Year for 2020!

Celebrating 25 Years with Mike In Jamaica!

Every company needs "A Mike!"

note from Michelle~

Mike has been with us for 25 years! Chuck and I remember interviewing him at our kitchen table when CSU was operated out of our Chantilly residence. He has helped us as a printer technician, depot technician, engineer, dispatcher, sales person and now Operations Manager.

Basically, he can run the company!

For his 25th anniversary CSU gifted Mike and his wife with an all-expense paid trip to Jamaica.

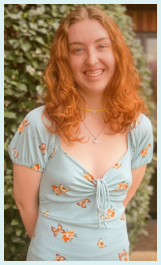
The photos are fabulous!

"Even the drinks are beautiful in Jamaica!"

cont. on pg 8

What's up at CSU?

Meet CSU's intern- Nina!



Nina is a local high school student preparing for college life as a sociology major. With her many talents and resourcefulness, Nina has been helping research and organize new clients, and is picking up new administrative skills that she believes will go beyond the four walls of Computer Services.

We are excited to have her here!

Having a Cheesy Time Celebrating National Grilled Cheese Day on 4/12!

The winner of the "Who Wore it Better" St. Patty's Day Competition is...

Melvin!

"I'd like to thank all my supporters, and give a special shoutout to Old Mill Pets."
-Melvin

Tune in next month for a cool story... *"15 Years in the Making"*

Our Services:

-Data Backup & Recovery
-Managed Services
-IT Consulting
-Network Security
-Cloud Computing
-Remote IT Services
-Cyber Security Training
-Mobile Device Management

We believe that experienced, reputable and fast responding IT support should be the standard.

CSU COMPUTER SERVICES UNLIMITED

Get connected with us!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Coffee Break:
www.csuinc.com/coffee

Digital Version of Newsletter:
www.csuinc.com/news