

INERVA INSIGHTS

Volume 6 • Issue 8 • August 2022

WHAT'S NEW



A New View On The Universe

The James Webb Space Telescope has been feeding phenomenal images back to Earth since early last month. Through its massive scale and ability to read infrared light, the hexagonal satellite is uniquely built to study the oldest parts of our known universe - the first stars and galaxies that ever formed. Because these objects are moving away from us as the universe expands, their light has been stretched and “redshifted” (appearing to shift to the red part of spectrum) and reaches earth as infrared light. Therefore, it takes a special machine like the **James Webb Space Telescope** to gaze into the past and read the data that has literally been warped by the universe itself.

UPCOMING EVENTS

Cyber Security Update 2022

August 16th 6pm FREE Webinar via Zoom

Cyber Liability Insurance for Healthcare and Associated Risks – Practical information from **Derrick Weisbrod**, CEO of **Inerva Technology Advisors**, and **Josh Barker** from **techrug** about:

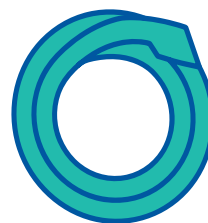
- Importance of cyber liability insurance protections
- Cyber security risks and methods used to compromise patient privacy and business cyber security
- The correlation between government regulations and NIST
- Cyber liability insurance and HIPAA compliance



This monthly publication is provided courtesy of Derrick Weisbrod, CEO of Inerva Technology Advisors

IN THIS ISSUE

- Page 2 – Educated Employees Are Major Security Assets
Tech Tip : How To Combat Negative Reviews
- Page 3 – Can Documentation Save You Time And Headaches?
- Page 4 – Cybersecurity Update 2022 - Cyber Liability Insurance



INERVA

TECHNOLOGY ADVISORS

Our mission is to be trusted advisors guiding businesses in the Greater St. Louis area with professional IT support that always maintains a human touch. We help local businesses to navigate these challenging times when new cyber security dangers affect us all.

EDUCATED EMPLOYEES ARE MAJOR SECURITY ASSETS

Forbes reports that businesses suffered 50% more cyber attacks per week in 2021 than in any prior year. That's 50% more chances for your employees to encounter a cyber-attack threat. Your organization will benefit if they know what to look for and how to stop a cyber attack.

Unfortunately, not everyone is as aware of the danger that businesses face in today's volatile cyber-attack landscape as you might think. An estimated 45% of respondents in a *HIPAA Journal* survey said that they don't need to worry about cyber security safeguards because **they don't work in the IT department.**



Even if an employee is aware that everyone is responsible for maintaining security, there's still a good chance that they don't know what to look for when it comes to spotting a cyber attack. Only an estimated 30% of internet users even know what ransomware or malware is.

Cyber security education works! Employees that are educated about cyber threats make better security decisions. Overall security-related risks are reduced by 70% when businesses invest in cyber security awareness training.

Get serious about security and compliance awareness training today. You'll enjoy lower risk and fewer cyber security incidents every day.

TECH TIP: HOW TO COMBAT NEGATIVE REVIEWS AND BUILD A BETTER ONLINE REPUTATION

As a business owner, you know that online reviews are important. A single negative review can damage your reputation and cost you customers. But what can you do to combat these negative reviews and build a better online reputation? Here are some tips.



1. **Respond to every review.** Positive or negative, responding to the review lets potential customers see that you pay attention to your customer's feedback. If you can answer a review personally with a reference to the customer or job you did for them, that will serve as a testimonial and make an even bigger impact!
2. Carefully read negative reviews and see if there is a way to resolve the situation. **Respond with humility and kindness.** Sometimes mistakes happen, and all you can do is apologize. But DON'T be afraid to call out a scammer who is leaving a false review! Potential customers read those negative reviews, and they notice when something seems fishy.
3. **Automate your follow-up process** to include asking your customers for reviews. The more good work you do, the more positive reviews will stack up, and the better your reputation will become!

CAN DOCUMENTATION SAVE YOU TIME AND HEADACHES?



The saying goes, “If it isn’t documented, it didn’t happen.” And while that may be an exaggeration, there’s certainly truth to the idea that good documentation can save you time and headaches. Documentation is an important asset for every business. It spans all aspects of your operation including your client list, billing procedure, data backup, and your login passwords. Any information that is vital to know in order to run your business is something that should be documented!

The reasons for keeping this documentation are as myriad as your business’s daily tasks. Having all passwords available negates the need to either write them down OR submit tickets to get forgotten passwords reset. The process of documenting often makes various procedures more efficient and repeating them becomes easier. Having a full list of credentials available will help you monitor when passwords need to be updated, and if one is compromised, it becomes easier to change all the credentials related to it. Having hardware documented assists with any repair or maintenance work and means that end of warranty deadlines and replacements can be tracked and planned for.

Many security frameworks require a full documenting of all hardware. Maintaining a list of data repositories to know where data is at all times is important, while documenting backup procedures is critical. There must

be a known path to follow in the event of a breach, loss of data, or disaster so that it is clear which assets need to be restored first in a crisis.

To make your documentation effective, it needs to fulfill 3 requirements: It must be **Relevant**, **Readable**, and **Retrievable**.

Relevant: If the process you need to learn about is how to upload a client’s document into a file share, then the documentation needs to be laser-focused on that task. Don’t offer alternatives or different ways to do it, only record the exact way you would want your newest hire to complete the task. This will make it easier to train new employees and easier for them to find the information they need.

Readable: Write your documents as clearly and precisely as you can. Don’t let them be too technical and complicated. Again, these should be used to train your newest employees! Include as much information as needed but try to keep it as simple as possible.

Retrievable: How you categorize and store your documents is as important as what they say. After all, it doesn’t help to have great instructions if you can never find them. Develop some simple rules for how you name your documents such as [User]_[Software]_Password and then keep the same structure! That way you will always know how to search for the information you need.

WHAT IS CYBER LIABILITY INSURANCE? DO I NEED IT? IS IT WORTH IT?

Our FREE Webinar will answer these questions.

We would like to invite you to the fifth webinar of our **Cyber Security Update 2022** called **Cyber Liability Insurance for Healthcare and Associated Risks**.

Derrick Weisbrod from **Healthcare Technology Advisors**, a division of **Inerva Technology Advisors**, and **Josh Barker** from **techrug** will be providing an update about the current state of cyber security issues and how you can protect yourself from methods used to compromise patient privacy and business security. Cyber liability insurance is crucial to that protection. Cyber liability insurance follows **NIST** standards when determining the risk associated with underwriting an insurance policy for a given business. The **National Institute of Standards and Technology (NIST)** IT security best practice standards are the basis for IT regulatory compliance that is known as **HIPAA** in healthcare.



Derrick Weisbrod, CEO of **Inerva Technology Advisors**, is a well-respected leader in the St. Louis community and a local expert in the IT industry. He originally launched **Inerva Technology Advisors** with the healthcare division called **Healthcare Technology Advisors** winning **Missouri's Best Award** for IT & Computer Services. Derrick is a past president of **Greater St. Louis MGMA (Medical Group Management Association)** and author of the book *Is Your IT Consultant a Liability?* He has also published IT articles in the *St. Louis Metropolitan Medicine Magazine*.



Josh Barker is the Senior Account Executive and Advisor at **techrug (The Technology Risk Underwriting Group)**. Prior to joining techrug in 2014, Josh owned a consulting company where he contracted with **J.S. Held** to provide independent loss assessment and adjustment services for numerous national and international commercial insurance carriers. Josh holds insurance licenses for both Property & Casualty and Life & Health products and is currently in the process of securing his designation as a **Certified Risk Manager (CRM)**.

Derrick and Josh will present our FREE Zoom Webinar on August 16th 6pm

CYBER SECURITY UPDATE 2022

Cyber Liability Insurance for Healthcare and Associated Risks

To register for this webinar, go to: <https://yez8q143.pages.infusionsoft.net>