INERVA INSIGHTS

Volume 6 ▪ Issue 6 ▪ June 2022

WHAT'S NEW

Derrick, our CEO at Desolation Canyon

Vacation Time!

Summer is rolling out its welcome and the world is turning slower in the long, hazy days. Many families head out on long-awaited vacations during the summer months. While it's great to get away, it's important to make sure your business is secure while you're at it! Social engineering hackers can use your vacation as a way to prey on your employees while you are out of town. Use common sense and don't post about your vacation while you are gone.

Does your staff know what to do if your business is hacked while you are away? Make sure you have solid security procedures in place, even when you're not there!

Our newsletter will help you with tips, info and updates about cyber security and the IT protection we all need now.

IN THIS ISSUE

UPCOMING EVENTS

Cyber Security Update 2022
June 21st 12pm-1pm by Zoom

Derrick Weisbrod, CEO of **Inerva Technology Advisors,** and **Al Alper** from **CyberGuard360** will discuss dark web monitoring, risk assessment, and vulnerability scanning. You will also learn about the effectiveness of employee cyber security training with pre-made video tips and accountability training dashboards.

For info go to: inerva.tech/free-cyber-security-webinar

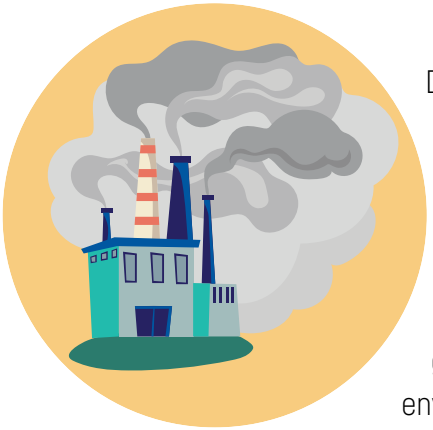
This monthly publication is provided courtesy of Derrick Weisbrod, CEO of Inerva Technology Advisors

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.

A DARK ECONOMY

The dark web is a major economic engine. If it was measured as a country, the dark web would have the world's third-largest economy, after the U.S. and China. That's great news for cybercriminals, but not very good news at all for businesses.



It is critical that businesses are sure they've got strong defenses in place that can help them mitigate the risk of trouble from the dark web.

Dark web monitoring is necessary now to prevent unpleasant surprises caused by compromised credentials.

Don't wait until the bad guys are on your doorstep with a compromised credential in hand that's going to get them inside your company's environment. Talk to your MSP (Managed Service Provider) about making sure that you've got your organization's credentials protected with dark web monitoring.

TECH TIP: TOP 3 WAYS TO PROTECT AGAINST RANSOMWARE

Phishing attacks and ransomware continue to be a method of choice for bad actors, often tricking well-intentioned employees into giving up data. There is no 100% effective method to prevent cyber attacks, because humans are always fallible. What are St. Louis professionals doing to lower their risk?

#1 – Updated, Business-Class Firewalls

This is the first line of defense, preventing hacking attacks that may target unprotected networks or take advantage of vulnerabilities not yet patched in the system. This is standard for any business, so speak to your IT professionals to make sure they are addressing all your needs.

#2 – Daily, Remote System Backups

Backups are the best way to restore your system after an attack or ransom event. Having working backups means that even if your network is attacked by ransomware, you can restore your system and lose only a day or a few hours of work. The alternative is usually to lose everything and start from scratch.

#3 – Cyber Liability Insurance

If a breach does happen, having cyber liability insurance can protect your business from litigation, help pay damages or fees, and even assist in paying a ransom to restore your data. No one wants to use their insurance, but in the current risk environment, it would be irresponsible to not have these protections for your business.

Call us today to find out if your business can access Cyber Liability Insurance: **314.312.4701**

COMIT: THE NEXT PATH TO SIMPLE, CLEAN IT

In many small businesses, people are expected to wear several hats. As an owner, you are probably also the human resources manager and IT director. And you do it well. But have you ever found yourself wishing you had more time to focus on the strategies and decisions that can help your business grow, rather than constantly putting out fires? Do you worry that your expertise isn't deep enough or wide enough to keep pace with your network as it grows? Is your IT team overburdened with regulations and constant small crises, rather than focused on long-term growth?

> ***"It was getting to be very difficult to manage the office as well as manage the IT."***

If you hire the IT director or more technicians for your team, that will burden your business with not only the cost of a salary and benefits but also the stress of finding and hiring new talent. Then you have to teach them your entire business. Consider this: **You could have an entire team, ready-made and fully staffed, at your disposal at a fraction of the cost.** You wouldn't have to source the talent, manage the workers, file the paperwork, or worry about hiring and firing them. That can all be done for you, while you focus on your in-house team and give them the resources, time, and flexibility they need to grow.

How can you do this? By entering into a Co-Managed IT (COMIT) arrangement. COMIT does not replace your in-house IT department, whether they are just 1 person or a whole team. COMIT simply takes the mundane, repetitive, and automatable tasks off your team's plate. Things like patch and log management, testing backups, and handling low-level service tickets take up most of your tech's time, but they don't offer the highest return. **Your people are your greatest asset** – if the office manager is spending half a day resetting passwords, are they really focused on growing the business?

Effectively utilizing your team's talents is the greatest asset of COMIT. Our clients at **Inerva Technology Advisors** were motivated to use our services by cyber security concerns, costs, regulations, and above all **TIME**. By employing a co-managing, partially outsourced model of IT services, you can save valuable time for your employees. They can then use their time and skills to better serve your business, all at a much lower cost than expanding your current IT team.

> ***"I was surprised by how easy the transition was and how reliable and quick the response time is for issues. Sometimes Inerva Technology Advisors can get things done quicker remotely than I can get done on site."***

COMIT is flexible enough to adapt to what your business needs. It can fill in the gaps of your team or bolster their support. Call Inerva Technology Advisors today to explore our co-managed options. No matter the size of your office, we can offer vital support that will help your current team work faster, be happier, and produce greater results.

We understand our local businesses, and we care!

During the busiest weeks of tax season in April, we delivered free pizzas for lunch to 30 lucky local CPAs, accounting firms, and tax prep businesses. Your business could be one of the lucky ones next year! To enter in next year's drawing, call us at **314.312.4701** or email us at **info@inerva.tech**.

HOW TO LEAD BY EXAMPLE WITH SECURITY AWARENESS

As the owner of a small business, you have a close relationship with your employees. They are aware of your actions just as you are of theirs. They see you as you check your emails, fiddle with the printer, take phone calls, and forget the password to your laptop… again. Your actions during the mundane work week can have a big effect on how your employees think of their job. Because of this, **your attitude towards cyber security can have a huge impact on how resilient your employees are** against cyber attacks, malware, and phishing.

Telling your employees over and over again to use secure passwords, check their emails, and not download attachments can start to fall on deaf ears after about a week. Constant repetition is not an effective training tool. **What works better is ongoing training that engages everyone with interactive tools and varied reminders.** If you, as an owner, set an example by initiating and attending training with your employees, the training will have a much greater impact on the office as a whole.

We all know that some security measures can get cumbersome and annoying - especially on the fourth time you've had to resend a two-factor authentication code! But do you curse and complain about the inconvenience, or offer a good-natured remark and complete the task? That attitude alone will affect how your employees think about the security measures, and whether they are likely to use them.

A comprehensive security awareness and compliance training program is a great way to set an example for your employees and engage them with training that works, while massively reducing the risk in your business. Companies that engage in regular security awareness training have 70% fewer security incidents. That's a significant advantage! Especially when you consider that **40-60% of untrained employees are likely to OPEN a malicious link** or attachment in their email.

Another way to engage your whole team in the effort to reduce security risks is by having a transparent platform that lets the team see how everyone is performing - even you! A dashboard that lets you manage employee training and accountability can let you easily track progress, assign needed training, and inform your team on their overall performance and goals. These regular training sessions can have a huge effect. **In just 3 to 6 months of training, the percentage of employees who opened phishing messages plummets from 60% to just 15%!**

You can kick-start your training by attending an upcoming **Inerva Technology Advisors** webinar where we will cover our new security awareness platform. Lead by example - sign up for it today and show your team your commitment to reducing your business's cyber security risk.

CYBER SECURITY UPDATE 2022

FREE Webinar Series!

Are You Sure You Are Still Safe?

June 21

12pm – 1pm

Derrick Weisbrod, CEO of **Inerva Technology Advisors**, and **Al Alper** from **CyberGuard360** will discuss:
Dark web monitoring, risk assessment, vulnerability scans
Employee cyber security training with pre-made video tips and accountability training dashboards

FREE DARK WEB SCAN AFTER YOU ATTEND THIS WEBINAR!

(A value of $150)

Check how secure your business is right now

For info and to register (or view previous webinars) go to: inerva.tech/free-cyber-security-webinar