The Tech chronicle

Cyber Attacks continue to RISE!!!

- As of March 28, the number of cyber-attacks related to coronavirus grew from a few hundred daily to over 5,000 in one day alone.
- As of May 2nd, the FBI Reported a 300% increase in reported cybercrimes.
- 71% of security professionals report increased security threats or attacks since the COVID-19 outbreak.
- Almost half (46%) of global businesses have faced at least one cyber security threat.
- In the next month, 49% of businesses expect to experience a data breach or cyber security incident due to a remote workforce.

June 2020

This monthly publication provided courtesy of Eric Stefanik, President of Elliptic Systems Corporation.

Our Mission: Building IT Security Awareness in Everett to Seattle with protective services like Cybersecurity, Business Continuity, Backup Disaster Recovery, VOIP, Cloud Computing, Virtualization and Managed Services.

This Is The #1 Thing You Can Do To Prevent Cybercriminals From Hacking Your Network

There is one thing many small businesses do that puts them at risk for a cyber-attack. They take a *reactive* approach to IT security. They wait until something bad happens before they do anything.

Unfortunately, we live and work in a time when you can no longer be reactive to cyberthreats. Practically every small business is connected to the Internet and relies on a network to function. It's the digital world we live in. We have to deal with hackers, data loss, equipment failure and everything else that goes with living in that digital world.

But you can reduce your risk and prevent hackers from getting into your network by taking a *proactive* approach to your cyber security and by working closely with an experienced IT services company that knows how to navigate today's digital world and all the threats that go along with it.

Looking back 20 or 25 years, reactive IT support used to be the norm. Something would go wrong and you could call up IT to fix it. Well, things are more complex in 2020. Threats take many forms, and simply being reactive doesn't work anymore.

What does it mean to be proactive with your IT support?

Continued on pg.2

Continued from pg.1

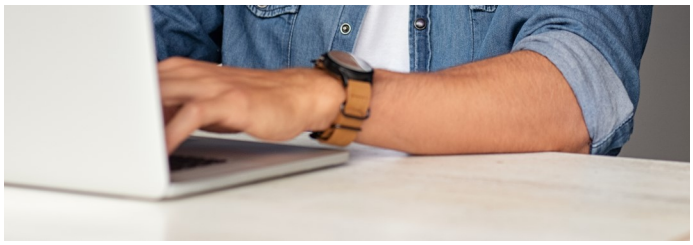
It means your business is more secure and you're ready to take on today's cyberthreats. It means you're working with professionals who have the tools and resources to protect you *before* the worst happens. It just makes sense.

Working with a dedicated IT firm means you don't have to take care of your IT security needs by yourself. If you're like most small businesses, you don't have the resources to hire an IT specialist or a whole IT department. Having an on-site IT specialist can be expensive. Because they are in such high demand right now, they command hefty wages.

Plus, you don't want any gaps in your support. If your one "IT guy" goes on a vacation or can't come in one day, you're out of luck should anything happen. When you work with an IT services firm, chances are they'll offer 24/7 support (many of the good ones do).

When you have 24/7 support, it becomes so much easier to catch problems before they happen. If your cloud backup goes down, you've got support. If hackers try to break through your network security, you'll be alerted. And all of your software stays up-to-date with the latest security patches. The list goes on.

"Working with a dedicated IT firm means you don't have to take care of your IT security needs by yourself."



You have people watching out for your interests. Think about how much better you'd sleep at night with that kind of protection guarding your business!

Here's another really great thing about working with a proactive IT services firm: you can tell your customers about it! In fact, you could make it a selling point. Today's consumers are more security-minded than ever before. And with data breaches hitting major companies every year, your current (and future) customers want to know that their personal and financial data are safe.

Don't wait until something breaks or until you are hacked before calling support for help. That puts the future of your business at risk. You need to work with an IT services company that is ready and willing to proactively manage your network. An experienced company has the training, certification and know-how required to tackle today's cyberthreats while managing your network's needs.

Make that call and never be caught off guard by threats that are never going to go away. Turn vulnerabilities into strengths.

Free DarkWeb Scan! Are your companies credentials for sale on the DarkWeb? How much do you know about the DarkWeb?

We are here to HELP! Find out if your company credentials are on the DarkWeb with our **FREE DarkWeb Scan**. The Dark Web is a hidden universe contained within the "Deep Web"- a sub-layer of the Internet that is hidden from conventional search engines. We go into the DarkWeb for you and keep you out of it so you don't add the risk of getting compromised.

Request your FREE DarkWeb Scan here or share this link ($79 Value):

https://www.escoffer.com/darkwebscan/

Simply call us at **425-441-9500** or e-mail us at Info@EllipticSystems.com

Email Phishing?

20 SECONDS TO BETTER EMAIL HYGIENE

1. WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS – Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

2. EXAMINE THE ENTIRE FROM EMAIL ADDRESS – The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.

3. LOOK FOR URGENCY OR DEMANDING ACTIONS – "You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

4. CAREFULLY CHECK ALL LINKS – Mouse over the link and see if the destination matches where the email implies you will be taken.

5. NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD – PHRASING This might be a deliberate attempt to try to bypass spam filters.

6. CHECK FOR SECURE WEBSITES – Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

7. DON'T CLICK ON ATTACHMENTS RIGHT AWAY – Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."

How To Turn Weaknesses Into Strengths

Public speaker and author David Rendall has a book called *The Freak Factor: Discovering Uniqueness By Flaunting Weakness* that presents the idea that your weaknesses can be flipped to become your strengths. It's all in how you view what you think are weaknesses and how you treat them. Rendall explains that rather than taking action in spite of your weaknesses, you should find ways in which they can actually be assets.

Rendall tours the country encouraging entrepreneurs and leaders to adopt this mindset. I've sat through his presentation a few times, and each time, I've come out with new and different perspectives. Here are my top three takeaways from Rendall's teachings and how I've applied them in my own life.

Change the situation, not the person.
You can't change people. You can compromise or accept them as they are, but you can't "fix" them. However, you can craft the situation to make it a better fit for that person (without forcing it, of course).

I've seen many companies make the mistake of promoting someone from within to a position they're just not meant for. Rather than forcing them into a position that's outside their wheelhouse, get them the things they need to be better at what they already do best. In other words, try looking at their strengths and finding the fit that's best for both them and you. They'll be happier and more engaged, and your company will run a whole lot more smoothly.

Surround yourself with other strengths.
No profitable business runs without the help of at least some other soul somewhere along the line, and those people who help us are almost always filling in a skill set that we don't possess ourselves. Why else would we ask for their help?

When you're building a team, think about your strengths and weaknesses. What are you not great at? What characteristics do you lack that you need someone else to fulfill? Conversely, what do you already have or know that would render another person with this same exact skill set useless? It's almost like putting together a puzzle. Find the people who fill in the gaps and complete the picture of your ideal company.

Cultivate your weaknesses.
The key thing that Rendall says is that your weaknesses are part of who you are, and you should embrace them and amplify them. What he means is that in the same way that you can't easily improve on your weaknesses, you also can't easily get rid of them, so why not accept them? As Jean Cocteau is often credited with saying, "Whatever the public criticizes in you, cultivate. It is you."

This is something we all have the capacity to do, but it's easier said than done because we are constantly advised to suppress those less-than-desired characteristics. The key is to sincerely harness your weaknesses and make them something constructive, something that you can use to your advantage or at least cleverly work around. From there, nothing can stop you from reaching any goal in sight.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Use These 4 Tips To Successfully Manage Remote Teams

1) Have a daily check-in. Whether it's over chat or video, check in with every member of the team. It might be one-on-one for certain projects or in a group setting if there are things everyone needs to know. Apps like Zoom make this a cinch.

2) Keep communication channels open. In addition to daily check-ins, let everyone know you are available throughout the day – and make sure you're available. Everyone must be able to communicate with you and each other. Slack is a great app for handling remote communication.

3) Look at results, not daily activity. Micromanaging never works with remote teams. When you take a hands-off approach, you want to look more at the end results of everyone's work, not what they're doing every hour or day. It just isn't productive.

4) Give your team the resources they need. If a team member is missing a critical piece of technology, such as a laptop certified to do the work that needs to be done, make sure they have it. Never assume everyone has everything they need. *Inc., March 16, 2020*

4 Business Intelligence Tools You Didn't Know You Needed

Reporting: Today's reporting software can track spending, sales, leads and so much more – and help it make sense. Companies like Una have software that turns your data into useful information.

Dashboards: They're another way to put your data in one place so you can make decisions. Domo, for example, offers a dashboard tool that brings your data together for utmost visibility.

Predictive Analytics: How is your market changing? With tools like those offered by SAP, you can get greater insight into what's next – and you can test models before making major decisions.

Data Cleaning: These types of tools clean your data to make it make sense. They get rid of outdated, duplicate or even false data points. Sisense makes tools that can accurately "fill in" certain incomplete data points, such as partial addresses. *Small Business Trends, March 3, 2020*

3 Things You Need To Stop Doing Online Now

Logging In To Accounts With Facebook Or Google: These buttons have appeared on websites across the Internet – including e-commerce sites. They make logging in a breeze. But as convenient as they seem, they're major privacy (and security) risks. They allow Facebook and Google to track your activity with greater ease. It gives them more personalized data they can sell to advertisers.

Saving Passwords In Your Browser: When you update or create a new password, most browsers ask if you want to save it. It makes signing into your accounts super-easy – but never say yes. This is NOT a secure way to store passwords, and it puts you at major risk.

Saying Yes To Cookies And Not Deleting Them: Websites now ask for your permission to "allow cookies." Cookies are used for advertising and website personalization. But they're also used to track your activity on the websites you visit. Every time you exit your browser, delete cookies first. It's one small way to protect your privacy. *Digital Trends, Dec. 6, 2019*