The Tech chronicle

What's New

We know it is a constant struggle to prevent the bad guys from accessing tools built into Windows while still enabling your end users to perform the tasks needed for their jobs but as the bad guys improve, so do we! We are excited to announce the roll out of a new cyber security tool which will provide an additional layer of defense for your business. After conducting extensive research and testing we believe this tool has enough granularity to offer up both protection and the access that your employees need. And it gets even better – key components of this new security tool will become part of our current security solutions at no additional charge. A strong defense is one of the best ways to protect yourself from a cyber-attack and we will remain vigilant in our efforts to improve yours.

July 2019

This monthly publication provided courtesy of Craig Covington co-owner Canon Capital Technologies

Our Mission

To enhance our customers quality of life and the health of their business

The #1 Security Threat You Face — And Top Ways To Protect Your Business From It

Cybercrime. It is more than a potential threat facing your business, it has become an unavoidable force of nature.

"It's like preparing for a hurricane or any other type of natural or man-made disaster that could create business continuity issues," says Theresa Payton, the Fortalice Solutions CEO in an interview with *Cybercrime Magazine*. "[It's the] same thing with a digital cyber-event." It can be easy to imagine this type of event happening to 'the other guy' but the problem is that cybercriminals go after *everyone*. They cast a wide net to generate the best results and advanced preparation is critical.

In fact, according to Roger A. Grimes 11-year principal security architect for Microsoft and cyber security columnist and speaker, "Eventually every company will be hacked." After decades consulting for many businesses, he's come to the conclusion that "every company is completely and utterly owned by a nefarious hacker or easily could be."

Owners of small and midsize businesses might imagine that they do not have enough cash or assets to justify a faceless hacker's effort but that assumption could cost you. The reality is around half of cyber-attacks target small businesses specifically. These types of attacks are not as flashy as an attack against a big bank or retailer and may not make the local news cycle but it's the attacks against small businesses that do the most damage. One 2016 study found that 60% of small businesses who have been hit with a cyber-attack closed

Continued on pg.2

within six months.

While it may seem like all bad news, there are preventative steps you can take to keep the bad guys out. Two of the best ways to safe guard against an attack are to keep all your software up-to-date and your team educated about threats. As Grimes puts it, "The two most likely reasons you will get exploited are due to unpatched software or a an incident where someone is tricked into installing something they shouldn't … every other exploit type in the world, added together, would account for 1% of the remaining risk."

> **"60% of small businesses hit with a cyber-attack closed within six months."**

The best way to keep your software up-to-date is to automate as much of it as possible. There are several tools built just for this and many programs will let you manage your software across your entire network from one location. Even better, most software is capable of updating itself. You'll still want to keep an eye on automated updates though to verify that they are actually completing.

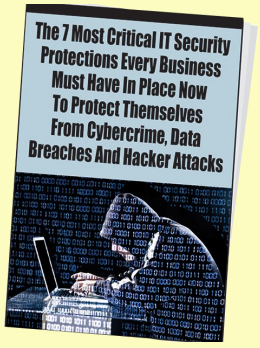
In order to avoid social engineering incidents you will want to put strong company policies in place. Be clear about your security plans and train employees about the dangers posed by malicious files and e-mails, among other things. Taking the time to educate your staff on the threats out there is your best line of defense against hackers. Education is critical and it begins with you as the business owner.

Communicate with employees about what they know regarding cyber security in addition to ongoing education. Continued education should update consistently as threats are always changing. The bad guys are constantly looking for new ways to break in!

Finally, you should partner with a highly trained, security-focused managed service provider or other IT organization dedicated to keeping you protected from threats. Some businesses try to manage this on their own only to realize that they don't have the resources they need. Others think they need an entire in-house IT team to handle all of these threats.

The reality is that by outsourcing work, you can save money while keeping the bad guys out and optimizing key parts of your network and software. It's all about being proactive. When you have a group of experts working every day behind the scenes, cyber security stays a top priority for your organization, whether *you're* thinking about it or not and it becomes one less thing you have to stress about.

FREE Report: The 7 Critical IT Security Protections Every Business Must Have To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks



Eighty-two thousand NEW malware threats are being released every day and businesses (and their bank accounts) are the #1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at www.ccmgtech.com/Cybercrime

Leadership Lessons Learned From The First Free Solo Climb Of El Capitan

Whether you think Alex Honnold's attempt to scale the massive El Capitan alone and with no ropes is foolhardy or transcendent, we all can learn a thing from his incredible feat. Honnold knew that to cement his legacy, he'd have to top the less intense (but still insane to any normal person) "free solo" successes of his past. So he prepared for two full years to complete the 3,000-foot ascent. As leaders, we should all identify with this – what will we leave behind when we're gone?

We can also learn from his thorough preparation. We need to think beyond "What will it look like to achieve our vision?" We need to think, "What does it mean for us to have a perfect run today?". Take the guesswork out of the equation as much as possible.

Once Honnold had his ideal outcome in mind, he practiced, climbing El Cap over and over and over again. In addition to full routes, he'd drill challenging sections repeatedly until it felt impossible to make an error.

For most leaders, making a mistake won't lead to death. But keeping this "deep practice" mentality in mind is essential for doing something truly great. Not many of us are going to have a Nat Geo documentary made about us, but we certainly can leave our mark on the world before we go.

Inc.com, 3/26/2019

Learn Like A Leader

Disraeli once said that all other things being equal, the person who succeeds will be the person with the best information. For leaders, learning isn't an academic pursuit. Leaders don't just learn to know more; they learn to be more. Learning is a critical means to this important end and how they find the ideas that fuel their ongoing improvement. Here's how the best leaders do it.

1.They make investigation and inquiry a way of life. Bill Byrne, featured on the cover of *Fortune* magazine as one of America's 1% wealthiest entrepreneurs, credits much of his success to his 15/15 program: he read 15 hours a week for 15 years.

2. They ask more and better questions of more and different people. The best leaders emulate the ancient city of Alexandria where no ship was allowed to enter the port without surrendering its books to be copied. They query everyone who passes into their lives, hoping to add material to their learning arsenal.

3. They think for themselves. Just because they ask lots of questions doesn't mean they accept what they learn at face value. Learn to consider what you learn with a healthy dose of skepticism.

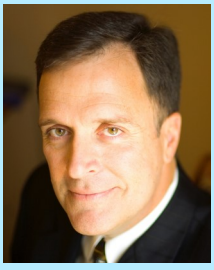
4. They choose critical thinking over conjecture. An important characteristic of the best is that they seek the truth. They want to act on factual information not speculation and conjecture. They ask, "How do I know this is true? Who says? How does it affect me?"

5. They learn in future tense. Study for the future, not the past. Develop your learning agenda on what you will need to know to be successful, not what you used to need.

6. They learn the most important stuff the fastest. When an area of knowledge becomes important, recognize the importance of that knowledge and glean the most important parts of it as fast as possible.

7. They design their own continuing education program. Unlike most people, the best design their own curriculum on an ongoing basis.

8. They listen to their intuition. As Robert Bernstein, former chairman of Random House Publishing, says, "In an age of information, only intuition can protect you from the most dangerous individual of all: the articulate incompetent."



Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an 'idea studio' that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of Fred Factor *and* The Potential Principle *and is a noted expert on leadership, team building and customer service. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out his books, video series, "Team Building: How to Motivate and Manage People," or his website, marksanborn.com, to learn more.*