The Cyberian Chronicle

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

cyberian
technologies

This monthly publication provided courtesy of Andy Banning, CEO of Cyberian Technologies.

Ransomware Protection. Guaranteed.
SentinelOne covers customers up to $1,000 per endpoint (up to $1M total) to recover files in the event of an undetected ransomware attack.

SentinelOne is recognized as a Visionary on the 2017 Gartner MQ for Endpoint Protection Platforms.

7 Ways To Dodge A Data Disaster

You stride into the office early one Monday morning. You grab a cup of coffee, turn on your computer and start checking e-mail…

A note pops up that rivets your attention:

"Your files have been encrypted. Send $5,000 within five days or they will all be destroyed."

You start sweating as your throat constricts and your chest tightens. Sure enough, every time you try to open a document, the same message appears. Your phone rings. It's Bob in accounting, and he's having the same problem. All files across your entire network have been encrypted. You are now a victim of Ransomware. You try and contact the local police for help.

They suggest you call the FBI. The FBI says they can't help you. What do you do next?

a) You pay the five grand, desperately hoping you'll get your data back, or…

b) You calmly call your IT pro, who says, "No problem, your backups are all current. No files were lost. Everything will be restored as soon as possible."

If your answer is "b," you breathe a sigh of relief and get back to work as your backup plan kicks in…

Ransomware attacks are more common than ever, especially at smaller companies. That's because small companies make easy marks for hackers. The average small business is much easier to hack than high-value, heavily fortified targets like banks and big corporations. According to Time magazine, cybersecurity experts estimate that several million attacks occur in the US alone every year. And that figure is climbing.

So how can you make sure you never have to sweat a ransomware attack or other data disaster? One sure solution is having a solid

backup plan in place. When all your data and applications can be duplicated, you have plenty of options in the event of an attack. Here then are seven ways to make sure you're in good shape, no matter what happens to your current data:

Protect endpoints across every threat vector. SentinelOne's Endpoint Protection Platform keeps user endpoints and critical servers safe from more than just fil-based malware. The platform detects the most advanced malware, exploits, script-based attacks, kills malicious processes, and quarantines infected files, making dwell time a thing of the past.

Tests backups regularly. Even though you may have spent a significant amount of money on a backup process, you can't be sure if that process works, unless you test and treat it like an unexpected circumstance.

Check backup software settings routinely. When new software or updates are put into service, a change in the way the settings are configured can cause incomplete backups, or backups that fail. Do the people who maintain your backups include this on their regular to-do list?

Make sure critical files aren't getting left out. As resources are added and priorities shift, documents and folders can get misplaced or accidentally left off the backup list. Insist on a quarterly or annual meeting with your backup management team to make sure all mission-critical files are included in your organization's data recovery systems.

Insist on regular, remote and Redundant processes. Typically, it takes 30 days for businesses to be up and running on local environments and about 5 days on off-site locations. We perform daily backups for both scenarios.

Address network issues immediately. Any component in your network that isn't working properly can introduce another point of failure in your backup process.

Every juncture in your network, from a misconfigured switch to a flaky host bus adapter, can hurt your backups.
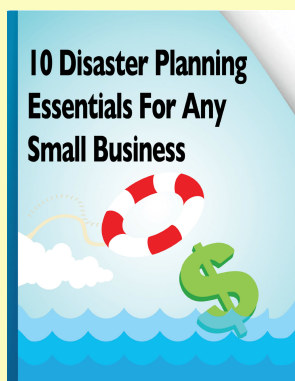
Ask for help with your data backup and recovery system. You cannot be expected to be an expert in all things. Yet data is the backbone of your business – its protection and recovery should not be left to chance. Leverage the knowledge, skill and experience of an expert who stays current with all the latest IT issues.

Data Recovery Review Reveals Backup System Vulnerabilities.

Don't let *your* company become another statistic. Just one ransomware attack can result in a serious financial blow if you are not prepared. Visit www.cyberianit.com TODAY or call (317)-401-6500 for a FREE Data Recovery Review. We'll provide you with a complete on-site assessment of your current backup system and prove how our new SentinelOne offering can provide further protection than you have in place now!

Are You Performing Periodic Security Assessments?

✓**Spam Email**- Most hacks start here. Protect your email.

✓**Computer Updates**- Keeping softwares up-to-date offers better security.

✓**Passwords**- Change passwords at least every 60 days.

✓**Training**- Keep users educated on security, hackers, and policies and procedures.

✓**Advanced Security**- Go beyond your anti-virus security systems.

✓**Encryptions**- Keep files encrypted on email and mobile devices.

✓**Firewalls**- Use a firewall to block unauthorized users.

✓**Backups**- Test backups to make sure they're saving correctly.

***Please reference the checklist data sheet included within this newsletter for more information.

The Misnomer Of Failure

So you think you're a failure, huh? Let me get one thing off my virtual chest right now: you're not. I realize you may be experiencing failure. You may have had a string of failures. You may have been told you are a failure. But it doesn't mean that's who you are. You are not a failure unless that's who you decide to be.

But before I prove you're not a failure, I want to share a personal story. Oh, and by the way, when I said "my virtual chest," I didn't say that because you are reading my article. I say it because my muscle definition is equivalent to Tweety Bird's. If that little yellow feathered turd and I got into a fight, he would own me.

I Am A Failure

My little story. In years past, I was an entrepreneur in the traditional sense, starting businesses and growing them. Today I am an author, which, not so interestingly, is just like any other form of business. You need to sell what you do and do what you do, really well. The only difference is, instead of having 30 employees reporting to you, you have one part-time assistant… who is either in India or is a family member or both.

I have failed a lot. I have lost all my money. I have crashed more start-ups than I have grown. I have offended probably everyone (including myself a couple times). And now I am failing at my fastest rate ever. Why?

If you asked anyone on the street – I mean anyone, including my mother – how "prolific" I am, they would say, "Who's this asshole you're talking about?" But here's the deal: failure is the ONLY way to success. Every day I take a shot at achieving my vision, and fail. And regardless of what your vision is, the only way you will get there is by failing your way to it.

Find Purpose

If you want to stop being buried by failure, you need to define your life's purpose. And if you don't know what your life's purpose is…your life's purpose (at least for now) is to find your life's purpose. Constantly ask yourself, why am I here? What do I need to do? And be willing to listen to the answers that you present yourself.

When you find your purpose, you'll get into the groove – where your hidden talents reveal themselves and you lose all sense of time. You're living your purpose when you build energy as you do it. You're living your purpose when you experience failure and you see it as another step up the ladder.

My Virtual Chest

In regards to my virtual chest situation, I am done with that bad failure, and am now a weight-room loyalist. Interestingly, I am now experiencing good failure constantly (those damn weights are heavy).

Tweety Bird can go suck it.

MIKE MICHALOWICZ (pronounced mi-KAL- o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford—a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for The Wall Street Journal; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book The Toilet Paper Entrepreneur. His newest book, The Pumpkin Plan, has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com/.

As of January 31, "outsiders" can now Skype into the White House Press Room. This enables journalists outside the Washington, DC, area to ask questions during White House press briefings. It's part of the Trump administration's strategy to keep in touch with people outside the beltway. Journalists attending via Skype must be at least 50 miles from the DC area. All political questions aside, it's just another example of business (or, in this case, government) taking advantage of available technologies. Or, in this case, finally catching up… Skype, the world's largest video calling service, is nothing new – it's been around since 2003. Sometimes it just takes a while for users to figure out how to make tech work to their advantage. *Yahoo.com, 01.31.17*

Anti-malware programs can't even touch this new kind of attack... "Fileless" attacks became all the rage among hackers in 2016. According to a report by cybersecurity firm Carbon Black, fourth quarter 2016 saw a 33% rise in these "non-malware" attacks compared to the first quarter. Experts expect the trend to continue through 2017. Cyberbad-guys carry out these attacks in any number of ways. Their "en vogue" method at the start of 2017 was hijacking PowerShell and WMI (Windows Management Instrumentation) to do their dirty deeds. Brian Kenyon, chief strategy officer for Symantec, said recently, "Fileless infections are difficult to detect and often elude intrusion prevention and antivirus programs." Reports show the Democratic National Committee hack last year used a fileless attack. *DarkReading.com, 12.27.16*

"DIY" data security kits can offer basic protection. Are you a do-it-yourselfer willing to take defending your company's data into your own hands? If so, you can find a variety of low to no cost products that provide basic safeguards. Koozali SME Server, for instance, bundles security and other server apps for small businesses. These include file sharing, directory access, redundant backups, firewall and web hosting. Its makers claim you can be up and running with it in less than 20 minutes. It's based on Linux, yet allows you to network Windows and MacOS as well as Linux-based devices. It's all free and there is no paid version. However, because no support is provided, you may need to contact a professional for assistance. *SmallBusinessComputing.com, 12.21.16*

Cassette audio tapes (remember those?) are making a comeback. Compact disk sales are declining, yet vinyl records have enjoyed a resurgence over the past several years. And last year, cassette sales rose to 129,000 units, an increase of 74% over 2015. So what's up with cassettes – why so popular all of a sudden? Actually, the numbers are still miniscule compared to the 105 million CDs sold in 2016. Yet the bump in cassette sales reflects a growing appetite for tangible items that fans can cherish. Also, it doesn't hurt that artists like Justin Bieber, Eminem and Prince brought tape reissues to market. Or that online retailer Urban Outfitters has exclusive deals to sell their cassettes, as well as vintage gear to play them on. *TheVerge.com, 01.23.17*