STRONGHOLD I.T.
Managed Technology. Redefined

Technology Times

"Insider Tips to Make Your Business Run Faster, Easier and More Profitably"

What's New

Stronghold I.T. is the premier Managed Services support Provider in London, Ontario; we are presently working with numerous organizations across South Western Ontario from many industry verticals.

Business IT Support plans include:

- Network Infrastructure monitoring
- Server and Workstation maintenance
- Next Gen Managed Endpoint Detection and Response (EDR)
- Backup Disaster Recovery Solutions
- Managed Security Appliance
- Cyber Threat Protection
- Service Desk

Stronghold I.T.
4-15911 Robin's Hill Road
London, ON N5V 0A5
519-471-9999

September 2022

This monthly publication provided by Stronghold I.T.

Our Mission:
To create and build professional, valuable and exceptional relationships with our clients; to develop and implement the most appropriate and effective technology solutions and processes.

Back To School!

The 4 Cyber Security Trainings You Must Do With ALL Employees

It's back-to-school season! Soon, our kids will return to the classroom, where they will relearn the information from the prior school year to ensure that they were able to retain that knowledge. There's nothing wrong with needing a refresher, and this is true for both students and your employees.

If your staff has not had a refresher course on your company's cyber security practices sometime in the last year, now is the perfect time to get them up to speed. After all, they can't defend themselves from cyberthreats if they don't know how. That's why it's so important that your team has bought into a cyber-secure culture and is aware of potential threats that could impact your business.

Cyberthreats come in all shapes and sizes, but an overwhelming majority of successful cyber-attacks can be attributed to human error, which is the main reason your employees need cyber security refresher training at least once a year. A lack of training can open your business up to hackers and other cyber-attacks by way of phishing emails, weak passwords, unsafe browsing and more – which jeopardizes your entire company. Additionally, in many cases, insurance won't cover your claims if your employees have not undergone regular training. Finally, customers usually don't want to do business with a company that isn't keeping their information protected. It doesn't matter how big or small your business is – you must make an effort to ensure that all of your employees have gone through cyber security training. However, if you've never trained your team on cyber security and are unsure of which topics to cover, don't worry because

Continued on pg.2

Continued from pg.1

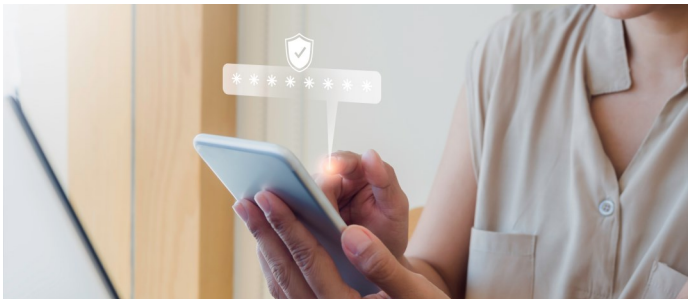
we've put together a list of the most important topics to discuss.

Password Security

Nearly every employee at every company has their own login to access the company's systems, data or Internet. When selecting the passwords for this login, employees need to use strong, unique passwords that utilize letters, numbers, punctuation and other special characters and are not shared between accounts. You should also ensure that your employees regularly change their passwords. For an extra layer of security, you can utilize multifactor authentication so you'll know that those logging in to an account are who they claim to be.

Email

Your employees should be cautious of any emails that come from addresses outside of the company. When your employees go through their email, they should not open emails from people they don't know or have not communicated with in the past. Unless they know exactly where the email has come from, they should not open any links or attachments within it.



Social Media

An employee's personal accounts should never be set up through a company email address. When posting on social media, your employees should be cautious about what they post in regard to work. They shouldn't disclose private information about your company or your clients on social media. If they did, it could be devastating to your company's reputation as well as your cyber security.

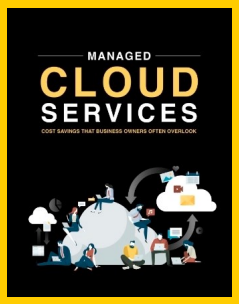
Protecting Company Data

At the end of the day, your cyber security practices are in place to protect company and client data, and your employees have a legal and regulatory duty to protect sensitive information. A reckless disregard for protecting company information can quickly cause your company to go under and has the potential to bring forth lawsuits.

Establishing strong cyber security practices and ensuring your team is aware of them through training is the best way to protect your business from cyberthreats. By implementing training on these four topics, you'll be on your way to developing a cyber-secure culture.

> **"Establishing strong cyber security practices and ensuring your team is aware of them through training is the best way to protect your business from cyberthreats."**

Moving To The Cloud Is More Economical Than you Realize



- What you stand to gain by outsourcing cloud IT support
- How to ensure unbeatable information security
- 12 underappreciated cost reductions attributed to cloud technology
- Why a cloud readiness assessment is critical for success

This content will help you get more value from your IT solutions by providing insight into what we've seen work for businesses like

Download your free copy today!

Get your FREE copy today at

https://www.stronghold.ca/potential-how-smbs-can-use-managed-it-ebook/

Security Terms Everyone Should Know

Malware
For a long time, the phrase "computer virus" was misused to refer to every type of attack that intended to harm or hurt computers and networks. The more appropriate term for these harmful programs and files would be "malicious software" or "malware." Whereas a virus is a specific type of malware that is designed to replicate itself, any software created for the purpose of destroying or unfairly accessing networks and data should be referred to as malware.

Ransomware
Don't let all other cyberthreats ending in -ware confuse you; they are all just subcategories of malware. Currently, one of the most popular of these is "ransomware," which is malware that encrypts valuable data until a ransom is paid.

Intrusion prevention system (IPS)
There are several ways to safeguard your network from malware, but an IPS is quickly becoming one of the non negotiables. An IPS sits inside your company's firewall and looks for suspicious and malicious activity that can be halted before it can exploit or take advantage of a known vulnerability.

Social engineering
Not all types of malware rely solely on fancy computer programming. Experts agree that the majority of attacks require some form of "social engineering" to succeed. Social engineering is the act of tricking people, rather than computers, into revealing sensitive or protected information. For cybercriminals, complicated software is totally unnecessary if they can just convince potential victims that they're a security professional who needs the victims' password to secure their account.

Phishing
Phishing is the act of defrauding people using an app or a website that impersonates a trustworthy or often well-known business in an attempt to obtain confidential information. Just because you received an email that says it's from the IRS doesn't mean that it is. Don't take such emails at face value — always verify the source, especially if the emails are requesting your sensitive data.

The Most Important Word In Business

"What's the most important mindset for success in business?"

I was recently asked this question by a video podcaster, and I carefully thought about my response. At first, I didn't think it was possible to identify the single most important mindset. I find questions that ask for "one thing" tend to oversimplify things. I considered that success usually depends on a number of factors and can't be broken down into one single mindset, but suddenly, it dawned on me: the one mindset that I have observed in successful vs. unsuccessful entrepreneurs countless times is generosity.

Oftentimes, you will see companies place honesty as their top mindset value, but in my opinion, that's putting the stakes a little too low. Companies shouldn't have to remind their employees not to be dishonest. You may also hear businesses putting kindness first, but kindness doesn't actually bring any value to their customers' lives.

Companies that put respect as their mindset are on the right path but still fall short of the benefits that generosity brings. To show someone generosity, you are giving them respect while also giving them something valuable. When you actually think about it, leaders who succeed are often generous. They're able to treat their employees, their customers, their shareholders and the community with a sense of generosity that brings them success. Those who fail to show generosity rarely succeed over the long term. Throughout my experience, I have met many business owners who have seen success and failure through their use of generosity.

I once talked with the CEO of a mortgage company who implied that his business succeeded by "tricking" low-income homeowners into signing up for mortgages that had hidden terms that were unfavourable to them. Once the housing crisis hit in 2008, which was caused by bad players, this guy's company and career were snuffed out under a pile of lawsuits.

In contrast, I remember talking to Ted Waitt, one of the co-founders of Gateway. I was blown away that a guy like Ted, a cowboy sporting ripped jeans, could create a multi-billion -dollar computer manufacturing company in the middle of South Dakota. Ted loved making technology less stressful for his customers while giving people good value for their dollar. His spirit of generosity was reflected in his company culture.

We often think that we need to do everything in our power to bring in more money, but adopting a mindset of generosity is better if you want to see success in life and your career.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

Improve Your Company's Culture By Maintaining Employee Happiness

There are certain businesses you walk into that just feel different. Everywhere you look, the employees are engaged, which is reflected in the way business is conducted. And their quarterly profits usually show just how much business is booming.

These businesses stumbled upon the secret that one great employee is often worth three average employees, and it's cheaper to pay these superstars 150% or more of the average industry wage to keep them around. These employees are flexible problem-solvers who can weather any storm.

However, you may have employees who quit because they weren't happy or adding value in their roles. How do you keep your other employees from following in their footsteps? One way is to set up an open exit where your employees give you a six- to eight-week warning that they are looking for another job. You can use that time to fill their role and train the new hire so there is no lapse in the transition period.

You can also pay your employees a better wage and offer benefits to keep them happy and engaged. When you work with these employees to make their lives easier, their flexibility becomes a gift rather than a burden. Unhappy employees can spell doom for your business, so do everything in your power to keep your team happy.

2 Scientific Methods To Prevent Memory Loss

It can be difficult growing older and realizing that your memory isn't as strong as it once was. You may try to eat supplements or do brain exercises on your tablet, but there are strategies you can implement to enhance your memory.

The first strategy is to aim for mastery, not relative performance. Researchers at Nagoya University in Japan have found that mastery-approach goals (i.e., developing your own competence) enhance memory of newly learned material, whereas performance approach goals (i.e., comparing yourself to others) can create "tenuous connections" in memory. The authors concluded the study by saying, "Motivation factors can influence inhibition and forgetting."

The second strategy is to simply ask why. A 2016 study from the *European Journal of Social Psychology* found that thinking more abstractly can actually reduce memory issues. The study examined how levels of "construal" (examination and interpretation) can affect memory, and their results suggested that "abstract thinking can eliminate retrieval-induced forgetting because of relational processing, demonstrating the roles of the levels of construal on memory inhibition." In other words, if you know the "how" and "why" behind things you intend to remember, you'll be more likely to remember them.