JULY 2022 | THE OFFICIAL NEWSLETTER OF JUST SOLUTIONS INC.

MAKE IT EASY

NETWORKS, PRINTERS, PHONES AND SECURITY

1997-2022 25 YEARS GREAT BUSINESS RESULTS.

SHIELDS UP!

7 WAYS TO IMPROVE YOUR BUSINESS' SECURITY POSTURE

You don't have to be a Star Trek fan any longer to have heard the phrase *"Shields up! Red alert."* It was repeated by Captain Kirk before every battle on the USS Enterprise. The United States government has declared "Operation Shields Up" for Institutions of all sizes. This was announced February of this year (2022). Yes, it coincided with the Russian invasion of Ukraine, but the US Cyber Command was already concerned with threats and hacker activity coming from North Korea and China.

Why does this matter to businesses like yours halfway across the planet? Shutting down an East Coast pipeline, our food supply chain or disrupting our financial institutions, keeps us preoccupied and distracted by world events. Ransom payments help fund more criminal activity. There are over 350,000 DOD contractors supporting our military infrastructure.

DAVID WOLF
VICE PRESIDENT OF JUST SOLUTIONS INC.

No business is immune to being a victim of a cyber-attack. Although not reported to news outlets, local companies are being breached every single day. Cyber liability insurance costs are doubling with the smallest policies averaging $10,000 a year. Getting a policy today requires security audits. Exaggerate your security posture and risk being dropped or worse, not covered even when you have a paid policy.

Continued on page 2

> **No business is immune to being a victim of a cyber-attack.**

Channel Futures. Leading Channel Partners Forward

MSP 501
2022 WINNER

WORLDWIDE TOP-RANKED MSP IN 2022

Here are the 7 cybersecurity protections you must have in place today. This is on top of the expectation you have already have a current, up-to-date firewall and the most recent managed endpoint protection (antivirus/antimalware). I am providing you this checklist so you can quiz your IT support team to make sure there are no excuses, and these solutions are in place!

1 Human Firewall – User Awareness Training

Teach your employees how to spot fake emails, scams, bad links. Test your employees by phishing them and retraining them when they get tricked. This is a requirement of the NY SHIELD Act.

2 MFA - Multifactor Authentication

This is the single, most important security feature you can implement to protect your business. Nearly ALL breaches involving ACH and wire fraud could have been prevented with better network and email security. Insurance companies know this and will demand you implement MFA for your insurance policy renewal.

3 Encryption

Encryption has gotten easier to implement and less confusing for your users. So now there is no excuse not to encrypt important, sensitive files or folders on your computers. When sending emails, send any attachments encrypted. By encrypting your emails, the messages including passwords you might share are now safe from prying eyes.

THREAT ACTORS ARE NOT SLEEPING. IN FACT, MOST ARE WORKING WHILE WE ARE SLEEPING!

4 Continuous Backups

Remember the daily, weekly, monthly backup rotation of tapes? That is now reserved for archiving. Considering the speed of change and the Internet, backing up your work continuously is a necessity. No business can roll back their activity to the day before. That could be thousands of emails, messages, file updates across dozens or hundreds of devices. Backups need to be continuous across all systems. Your backup is the ONLY recovery path against ransomware. How long will it take you to recover? The average is over two weeks or longer after a ransomware incident.

5 24x7 Log Monitoring (SIEM/SOC)

I just got a letter in the mail about my personal data being exposed to hackers from a breach at a local company. This breach occurred in 2020! I was just told June of 2022. I can promise you; the company was not monitoring their firewalls. How do I know for sure? They turned down my proposal for services. If no one is monitoring your network 24×7, then how do you know if you have been breached? According to the Verizon annual data breach report, every single breach could have been detected by a Security Operations Center (SOC) within minutes. The current average is over 8 months! Too late for a business to do anything but rebuild and recover. The damage is done.

6 SD-WAN (Software Defined, Wide Area Network)

This is a technical topic so let me simplify this for you. SD-WAN gives you duplicate, triplicate, quadruple Internet connections so your business never loses connection to the outside world. Yep, not just backup connections, but live, usable connections for faster Internet as well as redundancy. When you can't be without your VoIP phones, cloud services, email, or any Internet service, go with a "vendor" independent solution of SD-WAN. Never have all your "eggs in one basket".

7 Zero Trust Privileges

Stop giving your users admin privileges. They don't need them and should not be able to install updates and software on their computers. Keep that privilege limited to a select few. Zero trust limits bring your own device (BYOD) without proper protection and management. Geographic fencing will prevent remote users (probably in foreign countries) from accessing to your systems. Verify all devices, users, network connections regardless of where they connect. Segregate your networks and isolate key systems. Least privilege means only handing out privileges as needed and removing them immediately. We use a PAM (Privilege Access Management) solution for all our clients.

READ MORE ABOUT MFA

How can you stay protected when these threat actors have your passwords or pin codes you use every day on so many sites? The answer is additional layers of security beyond just a password. Multi-Factor Authentication (MFA) is an example of this layer of security. Continue reading *here.*

I realize this is a lot of information, but we are here to help you. We can implement any of the above measures for your business. We are happy to do security assessments, full audits, or reviews at a variety of price points. Don't put off security – the threat actors are not sleeping. In fact, most are working while we are sleeping!

Get your safeguards in place.

NYS SHIELD ACT
A BUSINESS REQUIREMENT

Make Compliance Easy

Reader Rankings WINNER

Rochester's #1 IT Support and Cybersecurity Company