VOLUME XI ISSUE 11
NOVEMBER 2020
OTTAWA ON


# TECHLORE

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

## INSIDE THIS ISSUE:



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
-Jim Stackhouse
NeoLore Networks

# Testing and Monitoring: What Challenges Businesses Need to Know

Most professionals and experts are focusing on establishing a well-structured data system to restrict data access, segregate data, and organize various operating systems for their business functions. IT teams can also help the business prevent breaches by designing effective solutions. These solutions include:

**1. Artificial Intelligence acts as a parallel in cyber-attack & in prevention**

AI has developed and transformed immensely during this era. With Artificial Intelligence, businesses can now set biometric login. After extensive data collection, modeling, and research, AI can now learn behavior patterns that businesses can use as a defensive tool. However, hackers can also use the same techniques for cybercrime.

**2. Technical skills gap**

A recent study by DCMS, or Department for Digital Culture, Media, and Sports, found that almost 653,000 companies in the UK cannot follow basic guidelines set by the government's cyber essential scheme. These companies make up almost 48 percent of businesses. They cannot follow best practices such as storing their data and setting up their firewall protection, etc.

The report claimed that approximately 30 percent of businesses, around 408,000 businesses, do not have any advanced cybersecurity skills, such as forensics, Pen testing, etc. Among them, 25 percent of organizations have already complained that this failure to build cybersecurity has lead to various losses.

In a report by the New York Times, it stated that there would be 3.5 million unfilled cybersecurity positions by 2021. In the face of increasing susceptibility to cyberattacks, we do not have enough cybersecurity professionals to help manage the risks. This is the biggest drawback in the future of technology. To navigate through these threats, it is crucial that organizations educate employees and bring in cybersecurity experts. The small number of institutions providing higher education and certifications in cybersecurity gives a glance at the upcoming disparity.

**3. Cloud Risks**

More and more businesses are transferring their data to cloud storage from traditional data centers because of the cost and flexibility. Businesses need proper security measures and configurations to move their data to a cloud system. If they do not create a proper barrier, they may fall into traps. Companies that provide cloud systems are securing the platform and infrastructure from threats of deletion and theft. Adopting these measures depends on the organization. Businesses can find various options such as VPN (Virtual Private Network), multi-factor authentication, and firewalls as solutions. Companies need to understand and implement various technologies and procedures to protect their business activities from internal and external threats.

**4. Ransomware Threats**

This type of cybercrime is increasingly popular nowadays. Using ransomware, cybercriminals can block or encrypt access to any network or system. After blocking access, hackers usually ask for money, depending on how critical the data is. Other than becoming a victim of data loss, companies also face a loss in productivity and finances. Later, they have to pay extra for IT costs, apart from legal fees. This can be a problem for many organizations.

**5. Internet Of Things (IoT)**

As more and more organizations adopt the Internet of Things, they face various security threats. These include ransomware and DDoS, which hackers use to access the organization's critical data.

## Fillup

Fillup™ is your very own Water Tower™, keeping a personal supply of water right at your fingertips. Our 70-oz. size holds a full day's supply, and Fillup's double-walled tank keeps water cold for 24 hours. Fillup can be used anywhere: on your desk, whether at home or in the office, on your bedside table, in your kitchen, on your back patio, and more. To learn more or to get yours visit fluidstance.com

VOLUME XI ISSUE 11
NOVEMBER 2020
OTTAWA ON

# Remote Access Tools: A Simplified Overview

As we live in a digital world, we can see remote work is on the rise. Even in locations where employees work and live in the same city, many individuals are choosing to work from home instead of going to regional offices. In a survey "State of the American Workplace," Gallup mentioned that in 2016, 43 percent of employees were working remotely from home offices; however, in 2012, the result was 39 percent. IWG has found that 70 percent of employees work remotely once in a week, globally.

**Supremo Remote Desktop**

Supremo remote desktop is easy to use and a lightweight application. This software needs no configuration of firewalls and routers to access the remote server or PC. In addition to that, you can use this software without even installing it. You can add multiple connections simultaneously on the same system. Furthermore, you will only need one license for an infinite number of computers.

You can install Supremo as a Windows service, which is an important feature. This feature enables you to launch Supremo automatically when Windows starts. You can use this software without any human involvement, controlled server, or PC. This means that you can instantly control the machine remotely.

**RemotePC Desktop Software Tool**

This software is a well-known tool for desktop use. This application helps you maintain a connection with your office or home system wherever you go without taking the device with you. You can easily print your information, transfer files, and manage them with a remote system.

Anyone can access their system to work on documents and presentations in real-time. Small organizations that want to connect their computer to a remote system prefer to use this software.

**Team Viewer Desktop Tool**

This is popular software in the innovative remote industry. Its main focus is cloud-based to enable online support through a remote system. Team viewer works as a catalyst to amplify and promote people's ideas and capability to overcome challenges and solve issues.

It's a whole package; you can rely on this software to share meeting applications and remote access that you can run on any system and mobile platforms. You can also download this software for personal use with a free trial version.

**LogMeIn Desktop Software Tool**

LogMeIn is leading software for remote connection that will provide support and connectivity solutions for all consumers and industries on small scale. Many companies use this tool to exchange their data and works remotely with more efficiency. With this software, access to all the information you need will be on your fingertips. This software will share, store, and collaborate with only one click. It has amazing end-point management, which will provide premier quality remote experience.

# The Perfect Back-to-Work Cyber Security Approach

After spending five months of lockdown, businesses are starting to reopen, and employees are back in their offices. But according to guidelines from health institutions, employees need to maintain a safe distance, stay sanitized, and practice other measures to protect their health that that of others. But besides SOPs, they need to start following better cybersecurity practices.

Disturbance due to COVID-19 will also affect businesses and technologies, and keeping a low profile on your security can lead hackers to intercept the office system and take control of critical data. Here are some cybersecurity protocols you should follow without any delays:

- Ask employees to change the passwords on all devices.
- Call the IT team to install patches and updates on all devices.
- Restrict the use of personal devices on office networks to prevent any possible malware.
- All your devices, such as computers, tablets, and mobile phones, should be scanned for any unauthorized applications.
- Also, conduct scans on all the endpoint devices.

# How SaaS Backup Can Help

If there's anything the last few months have proven, it's that life is unpredictable – it's important to be prepared for anything. In a world that increasingly relies on data, protecting it is of the utmost importance. In 2018, between 35% and 90% of data breaches were a result of human error. Accidental deletion, leaving unsaved work, and device loss or theft are just a few of the ways employees can be responsible for losing business-critical data. Small and medium businesses should rely on their managed service provider to advise them on a third-party cloud-to-cloud backup solution to ensure even in the most unanticipated circumstances. **To help SMBs Datto has created an infographic that be reviewed here https://bit.ly/3dx0Kbk**

# Tips for Online Privacy for Business Executives

1. Remove all profiles and details from public or office systems.
2. Avoid sharing your financial details on any shopping websites.
3. Always use unique and complex passwords for critical information.
4. Keep all your privacy settings on your social media sites turned on.
5. VPN is important for your privacy.
6. You should also use tracker blocking applications.
7. Avoid using public Wi-Fi devices.
8. Update the antivirus software on all your devices.


# The Importance of Cybersecurity Awareness for Businesses

By following cultural and workplace trends, we can understand why it is important to create awareness about cybersecurity among your employees:

1. Ten years ago, there was no concept of employees working from home. Now, many businesses are allowing telecommuting for various reasons. One reason behind remote working is to prevent cybercrime. Companies are adopting new policies and reshaping their organizational structure. This is allowing benefits like greater profitability and productivity.

2. Training employees to implement proper cybersecurity practices is no longer a process for a private organization. Many government institutions are also focusing on protecting their digital information and systems.

3. In an organization, a lot of employees are using personal electronic devices on the company's network, which can lead to a breach of security. Hence, many businesses are regulating the Internet of Things or IoT.

# Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an I.T security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyber attack.

Get the NeoLore Networks Cyber Security eBook for Free!

**It Features**

- Information on the various threats to your business
- NIST Security Framework
- CIS Controls
- Basic Controls

And More!

https://neolore.com/cybersecurity