WHO PROTECTS YOUR COMPANY FROM CYBER ATTACKS?

While it's impossible to plan for every potential cyber attack, a little proactive monitoring and maintenance of your network will help you avoid or greatly reduce the impact of the vast majority of computer disasters you could experience.

Unfortunately, I have found that most small business owners are NOT conducting any type of proactive monitoring or maintaining their network, which leaves them completely vulnerable to the types of disasters you just read about.

At a minimum, YOU SHOULD BE ADDRESSING THESE 4 CRITICAL COMPONENTS on a regular basis!

1 FIREWALL UPDATES

Are you subscribed to notifications from your firewall manufacturer, informing you of software updates? And do you update your firewall regularly?

2 BACKUP

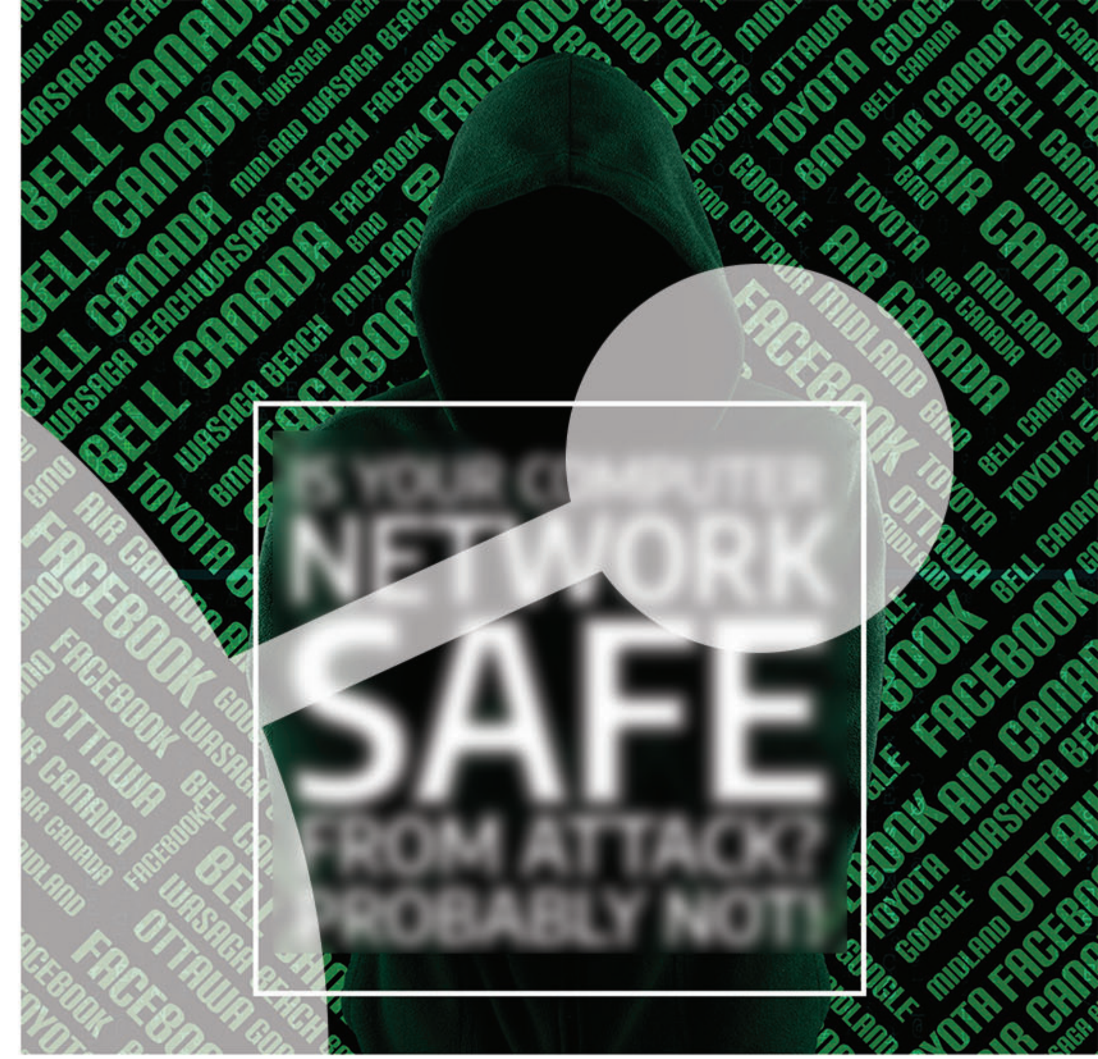
Do you backup your files every day? Do you check your backups on a regular basis to make sure they are working properly? Do you keep an offsite copy of your backups?

3 ANTIVIRUS

Are you certain that your virus protection is always on and up-to-date?

4 WINDOWS UPDATES

Do you update your system with critical security patches as they become available? Are you running the latest OS?



THIS IS PRIMARILY FOR 3 REASONS:

1. They don't understand the importance of regular maintenance.
2. Even if they DID understand its importance, they simply do not know what maintenance is required or how to do it.
3. They are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. That means no one is watching to make sure the backups are working properly, the virus protection is up-to-date, that critical security patches are being applied, or that the network is "healthy" overall.

BUT YOU HAVE TO HURRY...

We are only offering limited free assessments so fill out the form now to ensure your spot in line!

FREE

SECURITY AUDIT REVEALS THE TRUTH

This Free Security Vulnerability Assessment is valued at over
(1 Server and 1 Firewall)

NEOLORE

CYBER DEFENCE

THE WAY IT SECURITY IS SUPPOSED TO BE.

Please Visit www.neolore.com/am-i-secure and FILL OUT THE FORM to receive your FREE Cyber - Security Vulnerability Assessment.

VISIT US AT NEOLORE.COM
Lancaster Road, Ottawa, ON

THE SINGLE MOST **DANGEROUS** ASSUMPTION BUSINESSES MAKE ABOUT BANK SECURITY THAT CAN CAUSE THEM TO LOSE ALL THEIR MONEY

Here's a shocker to most business owners: Your bank often can NOT reclaim money stolen from your bank account due to fraud or cyber crime. That means if money gets stuffed from your business bank account from a hacker, phishing attack, identity theft or by any other means, you have little to no chance of getting it back.

This often comes as a surprise to businesses who think the Canada Deposit Insurance Corporation (CDIC) will "save" them from getting their accounts wiped out, and can get the money back once taken. The reality is that the CDIC insurance is to protect you from bank failure, NOT fraud, and only up to $100,000. So if your business debit card or account information gets accessed by a hacker and you don't notice quickly, you may be out of luck, check with your own bank if your are protected.

A recent study conducted by the National Cyber Security Alliance and Symantec found that 77 percent of small business owners in the North America think their company is safe from cyber criminals. The trouble is that 83 percent of them do NOT have a cyber security plan!

CYBER CRIMINALS

83% OF THEM DO NOT HAVE A Cyber Security Plan

DEAR 83%: CYBERSECURITY ATTACKS ARE INCREASING AT AN ALARMING RATE

WITHOUT A CYBERSECURITY PLAN

YOUR FIRM'S VULNERABILITY IS RAPIDLY INCREASING

WHY SMALL BUSINESSES ARE ESPECIALLY VULNERABLE TO CYBER SECURITY ATTACKS?

It's only a matter of time before the network crashes [gets attacked]. Ask NeoLore how this can be prevented.

1 Cybercrime is going up across Canada and most cases remain unsolved

2 The Nation Municipality victim of ransomware cyber attack

3 Foreign hackers targeting Canadian banks and government