5 Essential Ways
To Protect Your Business From CyberSecurity Attacks

In 2016, Cybercrime became the second most common type of economic fraud suffered by Canadian organizations*, with the Canadian Government estimating that 70% of Canadian businesses have fallen victim to a cyber attack.

Below is a list of 5 key strategies to protect your organization from CyberSecurity attacks.

“All You Need Is The Plan, The Roadmap, And The Courage To Press On To Your Destination”
Earl Nightingale

Train all employees

You have given the keys to your house and garden to everyone in your organization.

If you do not protect confidential emails you are leaving your organization, and your customers open to fraud, costly claims for not protecting data, and irreparable damage to your brand.

Forget the idea of a front door and a back door, there are many potential entrances to your house. That's before you make more entrances, letting customers / employees and others enter your house.

That is why you have to take your time!

Make sure you make it is a key part of your culture to train employees and to educate them on the best practices for protecting your organization from CyberSecurity attacks.

According to Indeed.com's 2017 Cybersecurity Report, Canada has seen its Cybersecurity skills gap widen significantly, scoring the worst out of the 10 countries assessed. With the ratio of cybersecurity job postings now far exceeding the number of skilled job seekers (1:0.68), it has now become more important than ever to bridge this skills gap through investing in high quality training and education for staff.

Protect Your Emails

A lot of organizations believe their live email security systems are up to the task of protecting their business from CyberSecurity attacks. Unfortunately, this is not the case. Many email security systems will not stop malware and phishing attacks, reducing an organization's security to zero.

Mistakes Can Be Expensive!
“The average cost of these cyber-attacks is estimated at $15,000 per incident.”

Organizations have been changing how they work over the years. Private communication networks are in many organizations and this helps to stop many points of failure.

The reality is every business needs to work toward a higher standard of quality, protection and overall email security.

It only takes one second to leave your organization vulnerable.

Recent Examples of CyberSecurity Attacks

Breach at UK government's Cyber Essentials scheme exposes users to phishing attacks

“An unknown person accessed a list of email addresses in a log file generated by the Pervade assessment platform and your email address, company name and the IP address of the Certification Body was on that list.” - June 2017

Canadian Parliament Shuts Down Emails Over Fears Of Hacking

“Commons spokeswoman Heather Bradley told HuffPost Canada the Parliamentary emails accounts "were temporarily deactivated as part of preventative measures" due to the hacking in the United Kingdom.” - June 2017

Blackout: The Other Russian Hacking Scandal

“FBI and Department of Homeland Security (DHS) officials believe that the hackers’ primary targets were nuclear power companies and other energy facilities. To date, those officials say, there is no evidence that plant operating systems have been compromised or that public safety have been placed in jeopardy.” - July 2017

Case Study: The Massive eMail Test

Over a 287 day period Mimecast tested 44,644 email users.

In this time period more than 40 million emails were inspected by Mimecast.

All of these emails were all passed by the incumbent email security system or cloud security service in use by the particular organization.

The Mimecast security inspections occurred passively after the incumbent email security system executed all of its security filters.

Overall the Mimecast security service determined that nearly 9 million of the more than 40 million emails, or 22.3%, were in fact “bad” or “likely bad.”

Not surprisingly, the vast majority, or 99.8%, of the false negatives that were passed by the incumbent email security systems and caught by Mimecast were annoying / benign spam email messages.

487 emails which contained unknown malware attachments were detected through the use of file behavior monitoring technology, generally known as sandboxing.

View the full report here.

Advanced Email Encryption platforms like Azure Internet, Sharefile, or Microsoft 365 emails will solve all your email security problems, giving you peace of mind and leaving you free to focus on running your business.

Your emails will be encrypted and can only be read by the intended recipients. Avail of features that will see hackers, and recipients sent emails in error, won't be able to see them. If you send an email in error, you also have the facility to recall it because you have full end to end control.

Create a SMART Password Strategy

Most people have many emails, variations, versions and manipulations of passwords protecting their most important information.

And, the list of accounts you are signing up to is always growing, each of which requires a password.

How do you track them all?

If you just use the same password everywhere, you are asking for big problems to come your way.

If you use unique, long, strong passwords with numbers/letters/special characters, then you will not remember them going into the future.

We can see the pain that people go through with their email security, and understand why they give up.

Don’t be fooled! This is exactly how your business will fail.
Here are two very easy ways to set up your passwords in order and save brain power and your organization money.

1. **Cloud-Based Password Manager**

What if your web browser remembered your passwords, automatically generated strong passwords and offered access to your passwords from anywhere?
That’s what you get when you use a cloud-based password manager like LastPass, — it bills itself as “the last password you’ll have to remember.” LastPass stores your passwords online in an encrypted form.

2. **Local Password Manager**

If you’re not comfortable storing your passwords online but still want your computer managing them for you, you can use a local password manager like Keepass. Keepass performs runs on your computer and doesn’t store any data on the web.

Penetration Testing & Vulnerability Discovery

Make sure to develop policies & procedures to identify security threats. On top of this, make sure to attempt to break your own system in order to truly understand your vulnerabilities. The easiest test to run in your organization to measure internal vulnerabilities is to conduct an internal phishing campaign against your own employees.

Rackspace
“We have seen positive results from our internal phishing campaigns that show the security education and awareness training is having an impact. We have seen a sharp decline in clicks on the bogus links and also more Rackers reporting the suspicious emails to the security teams.”

Work this into your own training programs and track the results.

Given the impact phishing attacks can have, such as changing your bank details as you invoice a customer, snatching your credit card details, and more, you and your organization must take every steps you can to protect your employees’ information.

Choose the route of complacency and you could end up facing class action lawsuits. CyberSecurity attacks will cost you time, money, reputation and clients.

Make sure you are not exposed to a Ransomware attack, losing all of your data, IP or earnings data. The trouble is. Security breaches are inevitable. So, always be ready.

"The bottom line is, CIOs [chief information officers] need to accept their company will be breached and shift their security strategy from 'breach prevention' to 'breach acceptance'," says Jason Hart, chief technology officer at digital security specialist, Gemalto.

Start Now. Don't Wait Until You're Attacked

The time to develop and manage a CyberSecurity strategy is right now.

If you wait until after you have been attacked, you will end up spending hundreds of thousands, even millions, of dollars to recover your organizations most important information.

Think about the above tips and work on developing a company-specific strategy that will enable your business to operate without the threat of an attack.

There are many different approaches, but the important thing is that you take action. Now is not the time for indecisiveness or passivity.

A Note To Our Readers

We appreciate you for taking the time to read our eBook. Did we miss anything you want to see mentioned in our next eBook, contact us at enquiry@cybersecuritybrain.ca with any questions.

We specialise in many areas of CyberSecurity and wanted to provide you with an overview of what you need to do in your organization, to help get you in the right mindset and to get you thinking about questions you want to ask us.

Our next eBook will look to provide a more focused approach, providing niche information on one topic in the CyberSecurity field.

Make sure to sign up to our newsletter on our website to hear about our next eBook before anyone else.

CyberSecurity Brain

Who are we?

CyberSecurity Brain, specialists in IT Security training and education, aim to tackle Canada's widening IT Security skills gap, in order to empower Canadian organizations to better protect their information from the ever-increasing threat of a Security breach.

Our goal is simple - to introduce high quality, instructor led Cybersecurity classroom courses that are led by genuine industry experts. By offering intensive, classroom style boot camps, CyberSecurity Brain aim to arm attendees both with the knowledge necessary to obtain some of the industry's most sought after certifications, while at the same time giving the attendees a set of practical skills that they can take back to their organizations.

Born out of frustration at the lack of high quality, practical classroom-based IT security courses, CyberSecurity Brain was founded by a group of IT Security Professionals who have come together to address this gap in the market and deliver what is needed – hands on, effective learning.

Changing the game – CSB is providing the highest quality classroom courses, flying recognised, industry leading instructors from around the globe to teach attendees and offer an all-round premium training experience.

Contact us with any questions.

enquiry@cybersecuritybrain.ca

CYBERSECURITY
BRAIN