7 MISTAKES
THAT MAKE BUSINESSES VULNERABLE TO BECOMING A CYBER VICTIM

Enjoy

CommsNet Group

INTRODUCTION

All kinds of organizations from government agencies to iconic consumer brands, Internet start-ups to trusted financial institutions have reported major data breaches in the last year.

We read that eBay the online retailer suffered one of the biggest data breaches whereby it compromised a database that contained customer names, encrypted passwords, email addresses and other sensitive data.

We also read in detail of the huge data breach involved with Target.

- 40 million credit and debit cards stolen
- 70 million number of personal records stolen
- 1 to 3 million number of cards that were successfully sold in the black market
- $53.7 million estimate income that the hackers received
- $200 million cost for reissuing 21.8 million cards

But how does it relate to a small business?

Symantec Internet Security Threat Report 2013, reported that any business no matter its size was a potential target for attackers. In 2012, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees: 31% of all attacks targeted them.

In the battle to keep ones personal and business information safe, its not just hackers one has to worry about, but lax security and stupidity.

- St Vincent Breast Cancer in Indianapolis send 63,000 letters contains appointments to wrong people
- Federal Credit Union accidentally attached file with information on 18,000 customers to an email
- Laptops or thumb drives were left in taxis that contained sensitive information

Keeping on top of the threat landscape is a constant challenge especially for a small business that is constantly juggling with multiple projects, priorities, cash flow, lack of expertise and time.

This article therefore highlights the Top 7 Mistakes that small business do regularly that leaves them very vulnerable to becoming a cyber victim.

MISTAKE #1
Assuming That You Aren't The Target

Surely hackers aren't interested in organisations like you and me, are they?

If only that was true! Gone are the days where you could sit, relax and not worry.

Did you know that 75% of attacks are opportunistic? If you leave your business door open, they will just jump in.

Worse still, you could be used as a route for an attack on one of your customers or suppliers.

It is also evident enough that by looking at some of the following statistics, it is clear to see that every user on the Internet is now a target.

- Only 1 in 5 emails are legitimate?
- Over half of the web traffic is coming from bad bots? These bots or zombies are scouring the Internet for application with vulnerabilities. Is your network vulnerable?
- Malicious websites grew by more than 600% in just 12 months. Moreover, 85 percent of these sites were found on legitimate web hosts that had been compromised.

Today, any device that is connected onto the Internet is now a legitimate target.

It would take approximately 2 hours for an unprotected Windows machine to be compromised once it is connected to the Internet ... and effectively owned. A Windows XP machine, could take around 20 minutes. Not even enough time to watch you favourite episode on the TV.

STEPS MOVING FORWARDS: Never assume that you are not a target! Place the appropriate security practices to ensure that your business is safe.

MISTAKE #2
Downloading Malicious Applications

People who would never dream of downloading an email attachment from a stranger, buy apps without considering the possible consequences.

Some applications are just malicious. They contain viruses, worms, malware or some other way of harming you. They might steal things like your personal information, others' contact information, or passwords and share them with others.

Did you know that 84% of organisations downloaded a malicious file according to the latest Checkpoint Security Report.

One of the most downloadable applications is the fake anti virus. Attackers are exploiting security conscious Internet users by tricking them into downloading and paying for anti-virus (AV) protection which is actually malicious software, known as 'scareware'.

Another very hot target area for attackers is the mobile smart phone.

The presence of malicious apps on Google Play and other popular Android app providers remains a persistent problem for Google. For those that have accidentally downloaded malicious applications are likely to receive annoying pop-up ads, have their personal information stolen, or be charged for certain services without their consent. But as a user, how would you know whether it is a legitimate application or not?

Social media also presents similar and increasing security challenges. Organisations like Facebook who are trusted by over a billion users expect their user profile to be secure. But there have been countless of stories with users being presented with legitimate applications but where it gathers your personal information or lead you to click to other sites that happen to be malicious or get you to download mischievous programs.

STEPS MOVING FORWARDS:

- **Ensure your computer has the appropriate security protections levels.**
- **Only download applications from reputable organisations including reputable websites.**
- **Look for evidence that the application might be fake.**
- **Do not respond to fraudsters asking you to download a security application because you they have monitored a problem with your computer.**

MISTAKE #3

Responding And Clicking To Unsolicited Emails

Don't you hate it when someone calls you unsolicited asking for a donation during the dinner hour? Or when your in-box fills up with so much spam you waste valuable work time sorting through it all.

When someone sends you an email with an attached Internet link, how do you know that this is a valid website and not a malicious one?

Often, these messages are sent with some exciting news. They are there to entice you and to lure you to click on that link. They are meant to fish you. That's is why it is called a "phishing attack".

Some of the most common characteristics these types of email messages have are:

- The address that appears as that of the message sender is unknown to the user and is quite often spoofed.
- The message does not often have a Reply address.
- An eye-catching subject is presented.
- It has advertising content. Website advertisements, ways to make money easily, miracle products, property offers, or simply lists of products on special offer
- They hope to trigger an emotions response causing you to act quickly.

Did you know that in Australia alone, over 20,000 organisations have been infected by a form of ransomware?

STEPS MOVING FORWARDS:

- **Never respond! If you do, they know that you are a real and live user.**
- **Never click on the "unsubscribe" option or other links within the email. It might be malicious**
- **Ignore headlines. Such headlines are often ways to entice you to visit a malicious website.**
- **Ignore messages asking you to visit popular websites requesting you to verify or change your preference. For example: Facebook is offering its users the ability to change its colour interface from blue to bright pink.**
- **Ignore messages that you have become an instant winner, overnight millionaire, congratulations awards, etc. These are all ways to get you emotionally involved to click the link.**
- **Ignore survey messages. They are just another way to scam your identity.**
- **Ensure your computer has the appropriate security protections levels.**
- **Setup an anti spam filter to capture majority of these emails before they arrive into your mailbox.**

MISTAKE #4

Accidentally Leaving Your Laptop, Smart Mobile Device, Thumb Drive In A Taxi, Car, Hotel, Restaurant, Airline Lounge, etc.

The rapid upswing regarding user requirements - useability and flexibility working environments has resulted in a swift change in the way users want to be able to access and interact with either personal or corporate information, from anywhere, at any time and from any devices.

However, the biggest risk with these smart and mobile devices is when they are accidentally misplaced, lost, or stolen. Such devices carry a trove of personal and corporate data and if not secured and land in the wrong hands, is a major source of data loss.

STEPS MOVING FORWARDS:

- **Consider encrypting all you mobile devices. Passwords are not enough anymore**
- **Remote wipe. If device is stolen, you can then issue a remote wipe the device.**
- **Ensure you have a backup of your mobile devices data.**
- **Consider using Mobile Device Management on all of your Smartphone and tablets.**

MISTAKE #5

Leaving Sensitive Information That Is Directly Accessible Online

Information disclosure can happen in an instant, be it the moment an employee posts an online message to their Facebook account, or walks from a car to the company building holding confidential data in plain view. The costs associated with such a disclosure are high and include financial loss as well as the loss of a organisation credibility.

All organisations, regardless of size, should be mindful of the need to protect their sensitive information by avoiding inadvertent disclosure online.

Here are some examples

- Accidental data leak helps wipe $22bn off Google's stock value. This was the result of the third-quarter earnings report that was due out after the market closed but was instead published on the Securities and Exchange Commission's prior to it being closed accidentally.
- The Australian Department of Immigration breached its obligations under the nation's Privacy Act when it inadvertently published the personal details of 9250 asylum seekers online.
  The department admitted it had accidentally made public a database of sensitive information including full names, nationalities, date of birth, gender and boat arrival dates of all individuals.
- Email addresses and encrypted passwords of around 97,000 users who tested early builds of the Bugzilla bug tracking software were left exposed for three months following a server migration

STEPS MOVING FORWARDS:

- **Preventing accidental disclosure is not as simple as restricting the set of applications with sensitive data to interact with another. Trusted application receiving data might share that data with another application that has unexpected disclosure. Hence, in a collaborative application environment, you will need to address the accidental disclosure problem as one of information flow.**
- **Identify your critical data and application assets and set appropriate policies of how the data can be utilised, viewed, configured, retained and exported**
- **Consider using tools that help users to identify and encrypt confidential data while at rest or when data is in motion.**

MISTAKE #6

Leaving Valuable Personal Details On Social Media Forums

There is a dark side to the Social Web, where Internet fraudsters and swindlers are determined to enrich themselves at your expense.

Based on the Consumer Reports magazine (June 2012—Facebook & Your Privacy), found that some people are sharing way too much, including an estimated 4.8 million who've potentially tipped off burglars where and when they're going on any given day and 4.7 million who've "liked" Facebook pages about health conditions that can be used against them by insurers.

Fraudsters are looking for clues online for any information that can be used for logins, email addresses, authentication, birthday dates, etc. This information is then used as an attack vector for gaining access to your bank or possibly sending you an email that contains malware, that when activated by you clicking a link or attachment compromises your machine.

STEPS MOVING FORWARDS:

- **Pay attention to what you post**
- **Keep personal information to yourself**
- **Don't post your organisation sensitive information**
- **Don't post password clues online**

MISTAKE #7
Using Obvious Passwords

According to Trustwave a well and respected global security corporation that weak or default passwords contributed to one third of compromises that they investigated.

The number one most commonly used password is "123456," and the fourth most commonly used is "Password." Your own name is also a common choice. So any password attacker and cracker would try these three passwords immediately.

So, what are the most common passwords? The top 10 list is as follows:

1 - Pet names

2 - A notable date, such as a wedding anniversary

3 - A family member's birthday

4 - Your child's name

5 - Another family member's name

6 - Your birthplace

7 - A favorite holiday

8 - Something related to your favorite sports team

9 - The name of a significant other

10 - The word "Password"

Naturally, if you used any of these ten to construct your own passwords, then you should probably take a moment to come up with something far more secure. After all, information such as birthdays, anniversaries and names can be easily researched using Facebook.

CORRECTION: Make your passwords memorable and unique.
Unique is the key here.

SUMMARY

You never want to be in the front-page news for the wrong reason. Finding out that your organisation just had a breach, your list of confidential clients along with their personal details stolen and as a result that your operations is no longer viable.

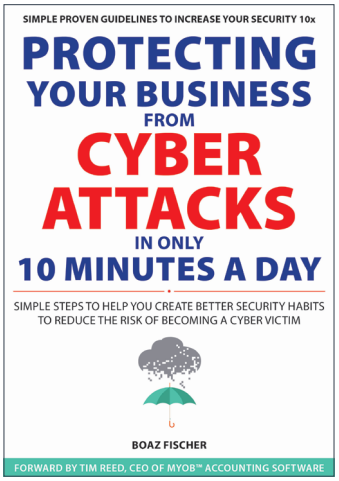
Did you know that 71% of compromises victims did not detect breaches themselves?

The number of breaches across the globe is ever increasing. Last year, it grew by more than 56% according to Trustwave. Majority of these attacks are financial motivated.

No matter where you are, as long as a criminal can make money by stealing and selling your sensitive information, you are fair game! So don't make it easy for them to succeed! Take security seriously! Don't lull yourself into false sense of security because you deem that you are not the target.

The threat landscape continues to evolve while the security strategies and technologies employed at many organisations are inadequate in the face of increasingly sophisticated and damaging attacks. Having said that, it is up to you to place some strong security habits to minimise your business risk.

Pay attention to the above 7 points made in this document seriously. Ensure that your organisation is well aware of the right security measures they need to employ on a daily basis.



If you would like to know more about how to improve your security online Boaz Fischer has just completed his new book ***Protecting Your Business from Cyber Attacks In Only 10 minutes A Day!***
www.protectingyourbusinessbook.com

Click here to reserve your 'pre-order' copy now and Save with Early Bird Special Offer!

ABOUT THE AUTHOR

BOAZ FISCHER has over 20 years of experience in the Information Technology field, having written over 30 articles, a book (two editions) specifically directed towards security best practices, presented and trained around the world. Boaz is also the CEO of CommsNet Group a technology company that helps organisations protect their Digital Crown Jewels. Boaz is a Master Certified in Neuro Linguistics Programming (NLP). Understanding human behaviour has played a major role in helping organisations develop empowering resiliency habits.