IT Security for Executives: Your Guide to Reducing Fraud

PROSERVEIT

Table of Contents

Why Cybersecurity?

Over 70% of Executives identify digital strategy as a top five priority.

So, how many executives admit that their company does not have an end-to-end security strategy? You're looking at 1 in 3. We all know that security is important, especially executives – we agonize over the what's at risk for your business, what's at risk for you personally. And yet, it's difficult to justify a spend or understand where to start as it relates to security.

One final thought. How many targeted cyberattacks does the average organization face each year? A staggering 186! Basically, almost every other day, your organization is under attack from somebody, trying to get to something, to get to your data, your information, at the end of the day, to financially negatively impact you and positively impact themselves. This is a very varied number, and includes all sizes of an organization, from SMBs all the way up to enterprises.

We feel that today's executives need to think about cybersecurity. Unfortunately, cybersecurity is something that all executives, regardless of your role or function, do need to be aware of and think about. And, depending on your role, the amount of thinking, per se, you need to do, will depend on what your responsibilities are. But it is important for all executives to understand.

When we think about statistics and how companies are thinking about security, when we talk to and when surveys are done around what are executives' top priorities, they identify digital strategy as a top five priority almost across the board – 70%, it's a fairly high ratio.

But, when we poll the same people and ask, "What percent of executives believe they are fully prepared for today's cyber security threats?", that answer is a more sobering 21%.

So, what percentage of executives have been able to fully fund the necessary investments to protect against modern security threats? You're going to see less than 25%.

21% of executives believe they are fully prepared for today's cyber security threats.

Less than 25% of executives have been able to fully fund the necessary investments to protect against modern security threats.

1 in 3 executives admit that their company does not have an end-to-end security strategyprises.

Top Cybersecurity Concerns: Two Different Lenses

When we think about cybersecurity, we see two different lenses. On the left – this is the "corporate hat" – this is what I need to do, as a custodian for my business. I need to help ensure that I'm helping to protect the people and data that I am a custodian for. I need to make sure that I'm protecting my customer data. You're protecting your organizational products, IP – basically your secrets. And, we do want to make sure that we're also securing any type of intelligent processes, so if your IP is less product-based and more knowledge-based, it's really important that all of that information is secure.

And if we flip here and put on our "personal hat", so to speak (and we'll describe why this is important as an executive to think about), we really need to think about how are we protecting identity? How are you protecting your family generation that may not be aware of the risks that technology exposes them to every day. And, of course, how are you protecting your finances? Because at the end of the day, what most of these people want is to have you write them a check, or give them a bitcoin, whatever the case may be to help fund their next attack.

So, what are some of your organization's security concerns and risks? And what are some of your personal or family security concerns and risks?

What is your executive team doing to protect security and privacy risks? And what are you and your family doing to reduce your security and privacy risks?

Top Cybersecurity Threats

- Protecting people & data
- Protecting customer data
- Protecting your product and IP
- Securing intelligent processes

- Protecting identity
- Protecting family members (elderly & young)
- Protecting finances

Final Statistics

You're going to see a lot of data that talks about the negative impact of a security breach on your organization. In the following slide, you'll see a lot of high profile, brand-recognizable names that have been compromised, and you're going to see things like, 160 million customer records compromised, and that's actually a really low number – I think that number there is from January to June of 2018, so only about 6 months.

160 MILLION

customer records compromised

229 DAYS

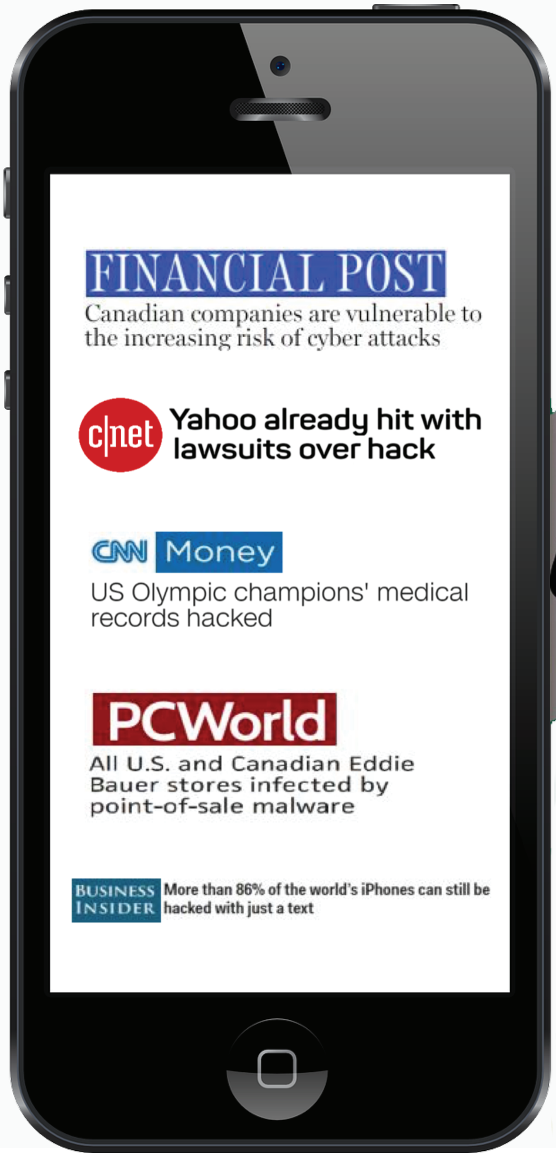
between infiltration and detection

$3 MILLION

of cost/business impact per breach

>$250,000

of cost/SMB impact per breach



FINANCIAL POST
Canadian companies are vulnerable to the increasing risk of cyber attacks

cnet
Yahoo already hit with lawsuits over hack

CNN Money
US Olympic champions' medical records hacked

PCWorld
All U.S. and Canadian Eddie Bauer stores infected by point-of-sale malware

BUSINESS INSIDER
More than 86% of the world's iPhones can still be hacked with just a text

Final Statistics

The second piece here, though, that's really important, and what we've seen as a trend amongst our customers is that, once a malicious person is inside your environment, their behaviour patterns are either one of two things. Either:

1. They're going to immediately do something negative to try and extract some form of money from you, so that's typically in the form of a ransomware attack. Basically where someone will come in and will encrypt your data and then they'll ask you for a set of money to give you the key to unlock your data back, and so they're looking to capitalize on that attack right away.

2. They'll stay engaged in your environment, and just snoop around. And basically, they're either trying to gather data that they can sell, or they're looking around to see if there's an opportune time to take advantage. For example, let's say you're trying to put your company up for sale, or you're looking to acquire an organization, or there's some pretty significant events that are happening – they're looking for ways to

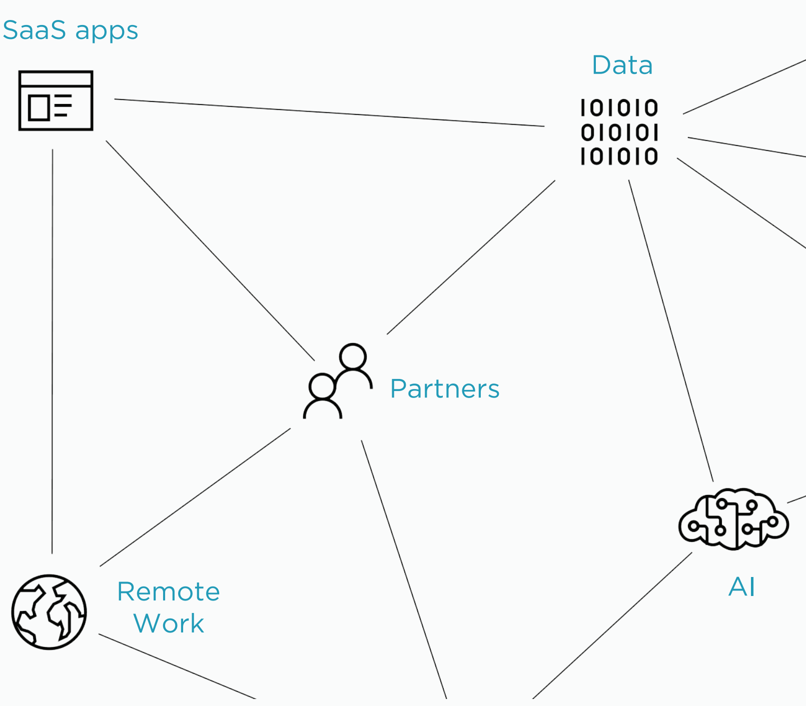
The last two numbers on this, both kind of on the upper end as an average – after all, when you look at a Yahoo, or a Target, or an Equifax and the numbers of records compromised, their costs will probably be far in excess of $3M. But even when you look at the average Canadian organization – and we see this among our customers, and we're talking organizations with $10M or less in revenue, the cost of the breach is significant – no less than a quarter million dollars is what we see every time, between a combination of loss of business, impact to reputation, opportunity cost for staff being down, any kind of services required to restore, and as well, anything type of thing needed as a post-incident restoring of brand reputation.

So, why is that? What’s been happening?

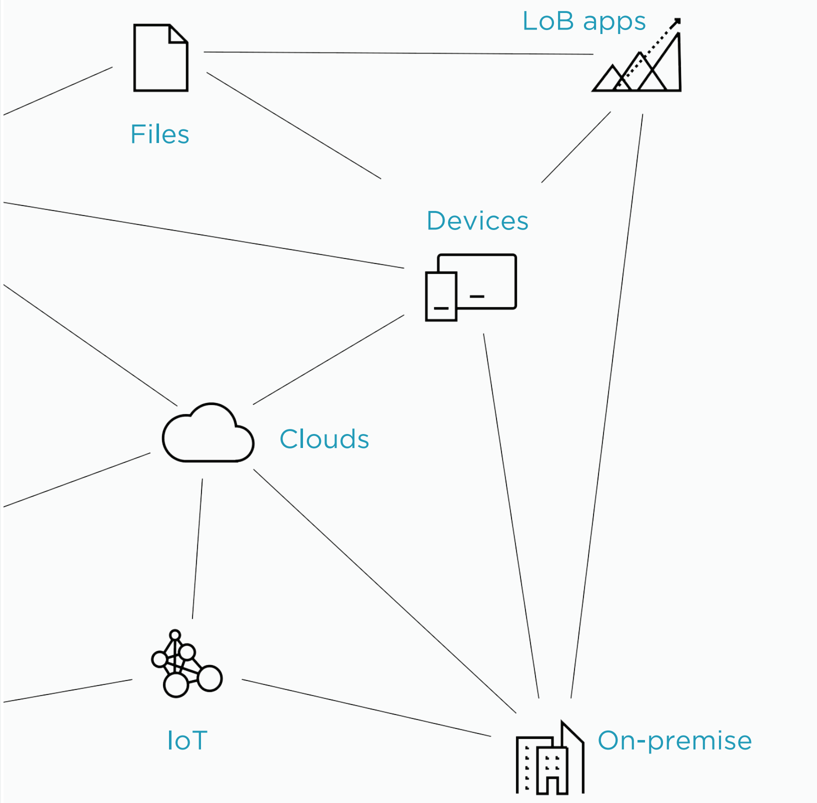
The reason the amount of attacks have increased is twofold:

1. What we do and how we use data now is dramatically different than a year ago, which is dramatically different than even five years before that. The rate of change inside of technology has been staggering – and that change is also happening to businesses.

2. And now, all of the things that encompass your organization is all over the place – you have data, you’ve got files, you’ve got devices, you’ve got remote offices, home offices, Cloud applications – and every single one of these things is a data point, that’s something for



Digital transformation has stressed your existing security practices



So, why is that? What's been happening?

When you think of that relative to the "good old days" – think of the idea of a castle.

At a certain point of time, a castle was the pinnacle of security – it's on high ground, with super-high walls, surrounded by water and hills. This was basically a virtually impenetrable castle, and the king of this land would have been able to protect everything that he held dear to him inside of these four walls.

Armies would come and go, and never could take it over. But one thing changed that significantly, and that was gunpowder. With the advent of guns and cannons, what was seemingly an impenetrable fortress was now a trap for all of these people stuck inside and it changed the game.

That change is what we're seeing right now. That change is happening because with the proliferation of the technology assets that we use, everyone uses identity or your information as the keys. Take this as an analogy – it doesn't matter how tall the castle walls are, or how deep the moat is, if someone has the keys to walk through the front door, they're in. And once in, they can basically do whatever they want. All of the thinking around security is based on the perimeter of the environment – not internally.

And that same thinking happens inside of a business's IT world as well – businesses take time to secure the perimeter – I'm going to buy the best firewalls, I'm going to buy the best anti-virus, and that's going to protect my business.

The truth of the matter is, that's not the case anymore, because that's not how people are attacking you.

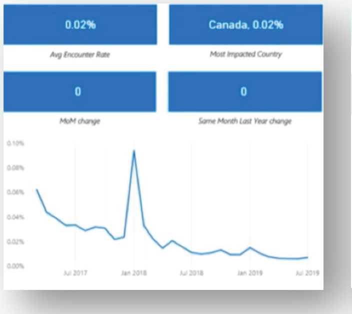
So, how has your security perimeter changed?

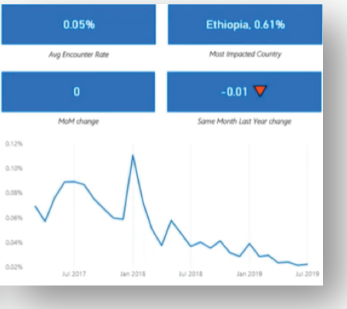
> When you think of your organization and all the technical things you have – where you have data, where you're connecting to the internet, the applications that you're using, the devices you're using to connect to – every single one of these things is an opportunity for someone to attack you.

The Data – Ransomware is a Downward Trend

So, we've mentioned Ransomware earlier – when an individual comes along and tries to install some form of software on your machine that locks everything out and they'll ask you for a ransom in return for unlocking it.

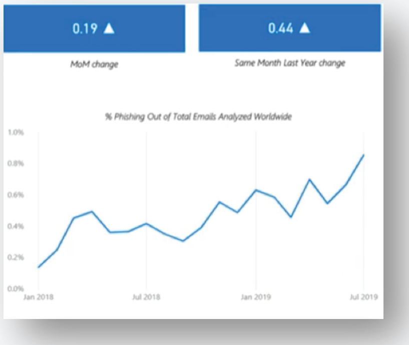
And where you see in this graph is some of the numbers around ransomware. The graph on the left shows that the global average encounter rate for ransomware is about 0.05%, with Ethiopia at a high of 0.61%. On the right is the chart specifically for Canada, and you'll see a significant spike around January, which was around the time that WannaCry came out. But one thing that you'll notice in either of these graphs is that ransomware is on a significant downward trend of what people are using to try and attack you.





The Data – Phishing is on the Rise

Think of the number of emails that you receive every day, trying to trick you into logging in somewhere and entering in your credentials so they can do something with them. This is called phishing. And this trend, as the graph below shows, is growing month over month, year over year, for the last three or four years.

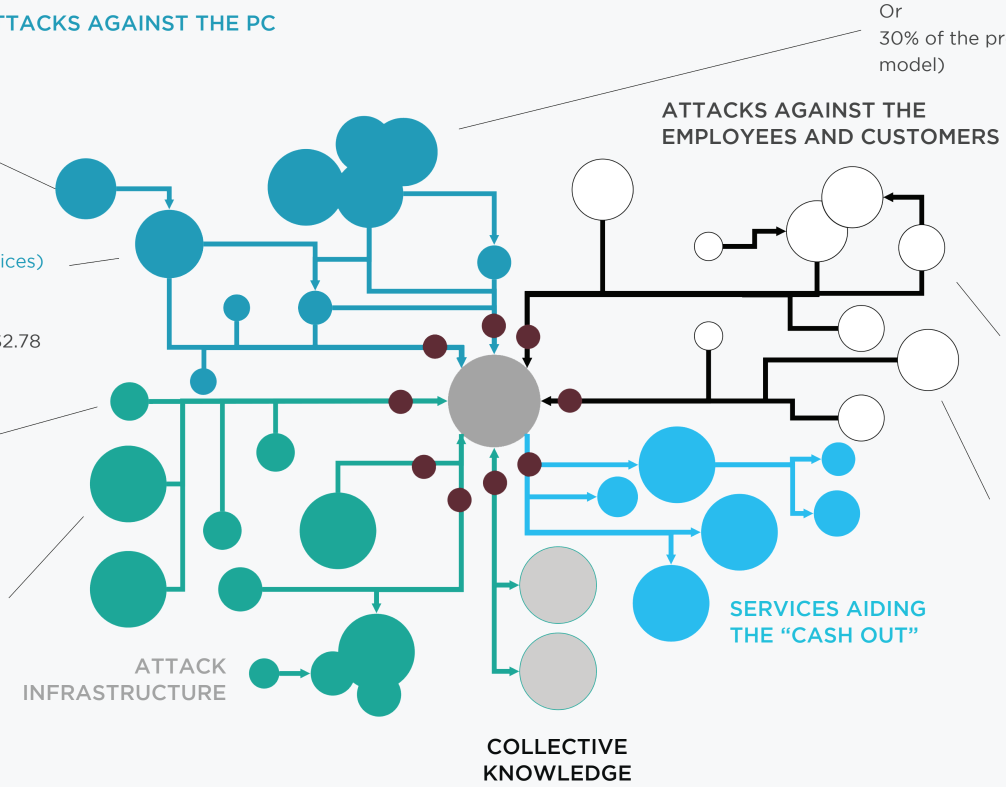


Why is that?

If we look back at our castle analogy, the best way to attack someone in the castle is to get the keys to the door. And, in a modern technology environment, the "keys to the castle", so to speak, is your username and password. So, if criminals can trick you into sharing your username and password, they've got the keys, and they can use them to their advantage. And, as the criminals have found out, this is a relatively inexpensive, but highly profitable and effective way of getting credentials.

Attack Services are Inexpensive

So, as this graphic shows below, attack services are inexpensive. It is actually really cheap – there's not a lot of money that threat actors will need to spend to gain access to things like breached credentials, or viruses, especially 0Day viruses (which are viruses that have not yet made its way into any anti-virus system, so most anti-virus software providers wouldn't have a defense against it).


ATTACKS AGAINST THE PC
ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS
ATTACK INFRASTRUCTURE
COLLECTIVE KNOWLEDGE
SERVICES AIDING THE "CASH OUT"

Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

Odays price range varies from $5,000 to $350,000

Loads (compromised devices) average price ranges
- PC - $0.13 to $0.89
- Mobile - from $0.82 to $2.78

Denial of Service (DOS) average prices
- Day: $102.05
- Week: $327.00

Proxy services to evade IP geolocation prices vary. As low as $100 per week for 100,000 proxies.

Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts As low as $150 for 400M. Averages $0.97 per 1K.

Source:

Why Identity-Based Security is Important

81%

of all hacking-related breaches use compromised credentials (people have paid for your credentials, OR you've used a commonly used password, i.e. Password123).

15%

of phishing attack victims fall victim a second time.

80%

of individuals use only 3 or 4 passwords across all of their accounts.

Let's look at these statistics in greater detail.

Most Commonly Used Passwords:

You may have seen the reports on Jimmy Kimmel or other talk shows that poke fun at the top 10 most commonly used passwords in the world. It's silly to think this is still the case, but a lot of the compromised credentials come from people using "standard dictionary words", or common, easy-to-find information like your last name tied to your child's birthday, or your anniversary date, or the street that you lived on as a child.

Unfortunately, everyone reading this eBook as an executive is a target. You are the custodian of your business. Depending on your role, you may have access to privileged information, access to company financial data, etc. These are the things that criminals commoditize, which makes each executive a potential target for a very targeted attack to get you do to something.

Phishing Attacks:

It's really important to recognize that it's an arms race out there. Criminals that are thinking of new and clever ways to get this information out of you are looking to make more and more authentic emails or attacks that will look very, very convincing around being authentic and having you follow through with what they're hoping you will.

Or, have you seen in the news, or seen those apps on your phone that make you look older? Digital aging is extremely scary, because that's like the worst-case-scenario around how people can impersonate you. How scary would it be, and how long do you think it would actually take technology to catch up to the point where you can take a picture of someone, and have an application mimic you so that someone could go on a "video call" and impersonate the CEO or the CFO of the company and ask someone in the company to transfer money on "their" behalf?

These impersonation attacks, like phishing attacks, are going to get more and more complex, and you, as an executive, need to be prepared for that.

Password: @TyaTaaB8

Password: @TyaTaaB88

Common Passwords Across Accounts:

You might have a series of passwords, so, let's say you've got a few "banking" passwords where you've used the same root word, but you've capitalized one, you've added an exclamation mark at the end of another, and you maybe added three numbers to the third. And then you've got a "work" password, where you've used a different root word, but you have a series of various add-ons, and when you're prompted for a password reset, you use the same root word and just change the 1 to a 2, the 2 to a 3, so even though you're complying with policy, but really, the password is the same, and it's very easy to attack.

The challenge with human psychology is that we're not really good at remembering things. So, unfortunately, because we're not very good at remembering, we'll use the passwords we use in our personal lives and use very similar passwords (or even the same password) in our corporate lives – again, the same root word, but maybe just a few variations at the end of it.

Important Criminals do understand human behaviour, and they're going to exploit our human nature around making passwords easy to remember.

Question from the Audience: Is it a bad idea to store your passwords on your iPhone in the Passwords and Accounts secure area?

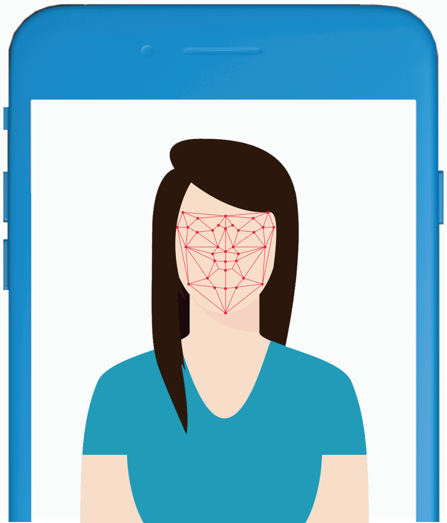
This is a good question. There are applications that are made for storing passwords and encrypting them in such a way to make them secure. We feel that those are good applications to use, with a caveat. It all depends on the Cloud Service Provider that is storing and encrypting those passwords – are they trustworthy? We look for an application that doesn't store the password data in their Cloud – we'd recommend that you look for an application where you can store the database of those passwords on something like OneDrive or Dropbox, where that thing is encrypted, but we're not at risk of some password provider being compromised.

Common Passwords Across Accounts: The LinkedIn Breach

To show why common passwords are a problem, let's look at a LinkedIn breach that happened quite a few years ago. All of those LinkedIn passwords could have been used as a starting point for threat actors to gain access to present corporate information. Here's why:

LinkedIn is a personal software use that was very tied to a corporate identity. Every single one of those people become targets; an attacker can tell where they worked, guess the email address of the company they worked for, and they actually have the target's password from that time to give them something to go and try and breach wherever the target is now, because that target is likely to use the same password because that's just human nature.

So, people use personal things in corporate world, and vice versa. Threat actors aren't going to try that for every single person, but as an executive or as someone in a position of authority, that makes you a target and worth the time to go invest some time and money into finding out your previous credentials (like finding out your old LinkedIn password) so they can bet on the odds that you're using a similar password (or the same password) in your new environment.



What Security Concerns are Keeping You Up at Night?

Let’s consider these 5 questions:

1 What would be the impact to our brand if we had a major cyberattack?

2 What happens if our data is accessed and violated?

3 What happens if your data/asset information are held hostage?

4 What is the risk to our employees or their family if private data is accessed?

- Think of things like employee benefits/health insurance usage, social security numbers, birth records, the ability for criminals to do impersonation and request a password on your behalf. As a company, we probably have a significant amount of data on our employees stored, and if that was stolen, identity theft could be a very real possibility.

5 What would be the financial impact?

How many of you can answer “Yes” to the following questions?

It’s been our experience that if you can answer yes to the first four, it’s highly unlikely that the fifth answer is going to be a “yes”, as well!

1 Do you know who is accessing your data?

2 Can you grant access to your data based on risk in real time?

- To determine this, let’s look at the “credit card” example: you make a purchase one time, and then an hour later, you make another purchase from halfway around the word – this is almost physically impossible for you to make two purchases, so it’s pretty clear that the credit card is going to limit access to your card based on risk in real-time. When an employee logs in from the office, and an hour later, they log in from Hong Kong, it’s pretty clear that one of them is not the legitimate user.

3 Can you protect your data on devices, in the Cloud, and in transit?

4 Can you quickly find and react to a breach?

- Unfortunately, we deal with this on a monthly basis, where a customer of ours falls victim to a phishing attack, where their credentials are harvested, and from there, a criminal is able to use those credentials to gain access to things they shouldn’t. The reaction time to those breaches can be critical to stemming the losses.

5 Do your users love their work experience?

How Many of You have Had “The” Chat With Your Children?

It’s important to protect not just yourselves, but your family, as well. We encourage people to think about them as additional attack vectors for people who really want to get to you. If you’re in a high-profile position, your spouse, your children, or your parents could become a target for threat actors. It’s not fair – what did they do wrong? – but it’s a reality. You need to understand, and help your children to understand the risks that are out there, and potential risks they could be exposed to.

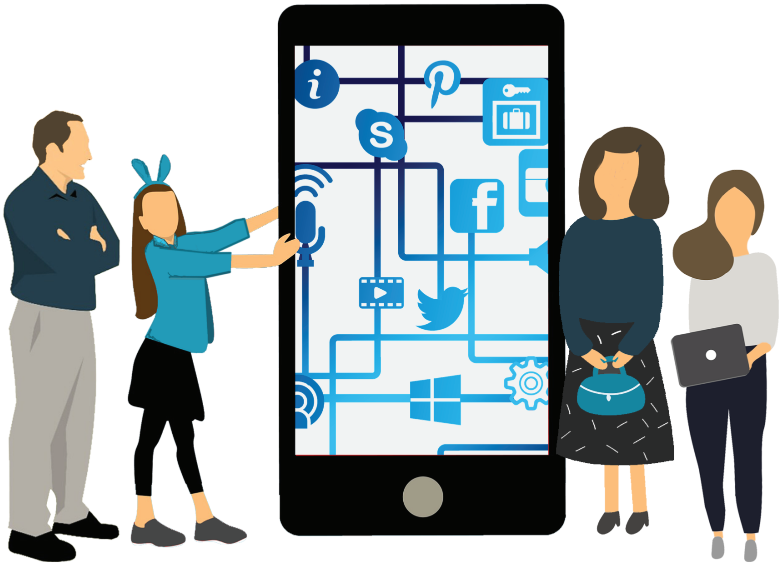
1 If you wouldn’t do it face to face, don’t do it online!

2 Once you’ve written something online, it can’t be deleted!

3 Become friends and contacts in your children’s social networks – but also keep an eye on what their other friends are doing.

4 Think about technology the same as a pet – it needs care and feeding!

5 What would be the financial impact?



Your Security Checklist

□ Identify corporate data crown jewels

□ Create your corporate and personal security standards

□ Corporate and Personal Multi Factor Authentication

□ Corporate and Personal Password Safe (KeePass)

□ Breach detection services

□ Identity monitoring solutions

□ Run threat simulations

□ Education share what you are learning!

□ Perform a self search quarterly!

□ Flash Drives (to use or not to use)

□ Personal/family and corporate password policies

It's important to make sure that you have a "mini-checklist" of things to look at inside your digital organization:

- From a security perspective, it's important to understand what your data "crown jewels" are. What do you want to protect – what's important to you?

- It's also important to understand what your corporate and personal security standards are. For example, password behaviour. The National Institute of Standards and Technology (NIST) recommends not using passwords but pass phrases. They also recommend not using password expiration policies in an organization, because it provides a false sense of security, because, as previously mentioned, people basically keep the same root password and just change the numbers and/or symbols each time they're forced to change their password.

- This is where **Multi-Factor Authentication (MFA)** comes in – enabling MFA provides an additional layer of security. At a bare minimum, all of your personal and corporate banking applications, your main email account (gmail, Hotmail, or whatever you use), and anything else that's private and important should have MFA enabled.

- Have a corporate and personal password safe. We recommend using an app (like KeePass or another similar app) that you can download for your phone or PC – as long as it's professional or trustworthy.

- Look at breach detection services.

- Think of your monitoring solutions.

- Look into threat simulations, so that you're ready for potential breaches and attacks.

- **Education** – you need to share what you're learning. Make sure that people in your organization are aware of things like phishing attacks, and how to protect themselves.

- Perform a **self-search quarterly.** There are several online tools that will allow you to search yourself and see if you've been a part of an attack. For instance, the website, have I been pwned? is one that allows you to enter your email address and it will tell you if you've been a part of a compromise in the past. If your email address does come up, it's a sign that you should at the least, change the password that's associated with the email address, and also change any passwords that you've been using that are similar to that compromised password – especially if it's used in a banking situation.

Do you have an end-to-end security strategy for your organization?

Our Executive Cybersecurity Workshop will take the concepts in this eBook and provide further depth to them. You’ll:

- Review the top cybersecurity concerns for your organization.
- Understand your personal and corporate risks.
- See how you can improve your security habits and behaviours.
- Receive a security checklist similar to the one we’ve already shared but customized to your business, based on the discussion we have.

We’ll be able to cater this in a little more detail to your specific organization, and help your business understand what is at risk for you and your business, both from a personal and a corporate life, then determine how to create a security checklist that’s customized to your business based on the conversation.

PROSERVEIT
MAKING TECHNOLOGY TRANSPARENT

www.ProServeIT.com | Cloud@proserveit.com