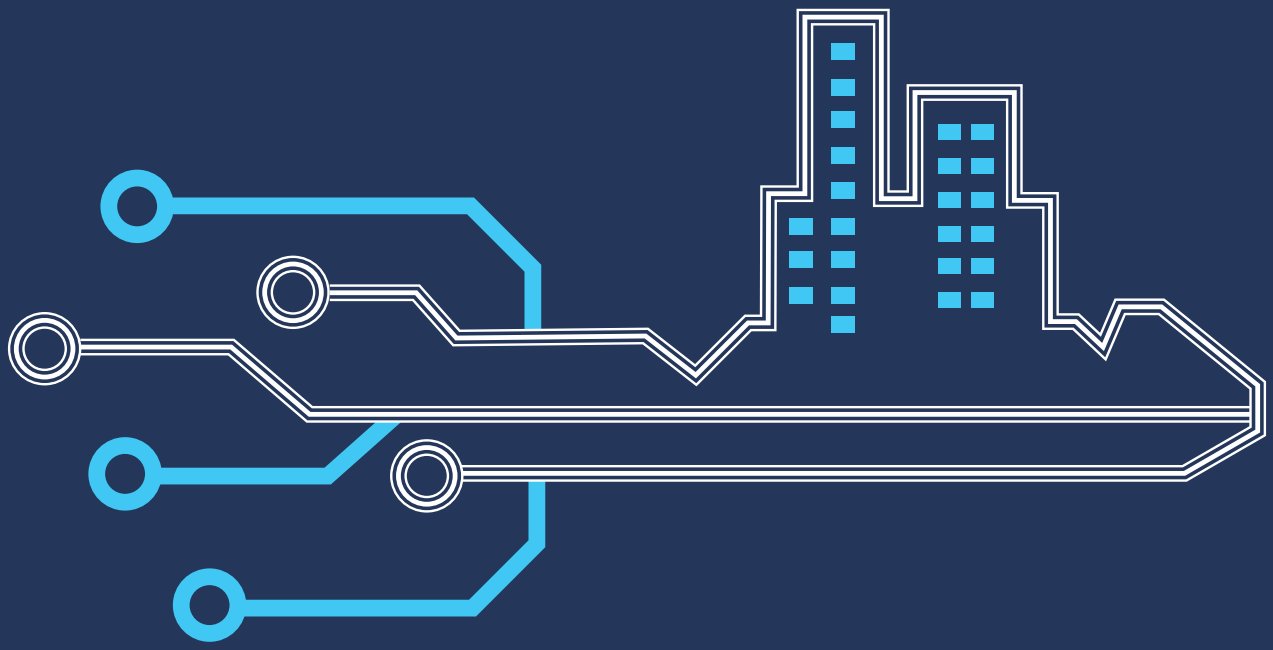
Performance
Advantage

PRACTICAL GUIDE SERIES: DATA ANALYTICS



THE BUSINESS GUIDE TO CYBER SECURITY

TABLE OF CONTENT

Introduction 2

The Business Guide 3

The Business Case 6

What kind of threats are out there? 9

You don't have to do this yourself 13

Cyber security is a hot issue. But why is it important to someone who runs a business? Because you've worked hard to build your business. To serve your customers. To win new business. Yet it all can be stolen from you. Years of hard work down the drain — if you don't understand the business impact of cyber security.

The reality is that there is an enemy out to get you. Sooner or later, every business, regardless of size or industry gets hit. It can be a hacker. Malware. A disgruntled employee. Hardware or software failures. Or as we see more and more — it can be strictly business.

It sounds incredible but it's true. Online fraud, holding data for ransom and other cyber crimes are now a growing multi-billion dollar world wide business. And businesses of every size are their new target markets.

The odds are not in your favour. With the double digit growth in this new "industry" every business is or will be affected.

The impact? If you fail to prepare properly you can get hit in three key areas:

- **Financial loss**, whether in actual dollars stolen or the cost of dealing with the issues these cyber-crooks create for you.
- **Loss of customers** or sales whether its from business interruption, bad publicity or just your inability to meet the security standards that customers demand.
- **Regulatory penalties** from failure to meet government standards. All it takes is one complaint to a government department and you can be in for a world of hurt. Ever faced a compliance audit for taxes or Workman's Comp or other government regulation? Security is the next one and like any government audit — even if you escape the fines — you don't want to go there.

It's not fair that you work so hard and have someone take it all away. The good news? You can fight back — very effectively.

THE GOOD NEWS

Even in a world of threats you can still survive and thrive by taking some basic action. It's no different than protecting yourself against any risk. You buy insurance. You put in alarm systems. You train people to stay safe.

It's the same thing in the world of cyber-threats. You can't fix every risk, but if you follow our guide you can vastly reduce your exposure, increase your ability to recover and make an effective case to regulators that you have done what is needed.

THE BUSINESS GUIDE

We created this guide and aimed it at business managers and owners. It's short, factual and practical. It will give you the basics that you need to understand why cyber security is important and what you need to do. It's not "for dummies" — if you've built a business, you are no dummy.

It's written in the language of business, not "techno-speak". And we did that intentionally because while some technical skill is required, you are the one who knows your business.

It's about protecting your business.
We know that you want to protect your business. Despite that, it's also very clear that many businesses don't take cyber security seriously enough.

A 2018 Scalar Security Study (commissioned by Scalar and conducted independently by IDC Canada) showed that Canadian organizations are attacked in varying degrees of severity more than 450 times per year, with 87% suffering at least one successful breach. Almost half (46%) are not confident in their ability to defend against attacks.

Here's some further information from that study — again, an independent study conducted by a very respected research company:

- Of the companies that suffered a security breach, 47% had sensitive data stolen.

87%
Canadian organizations are suffering at least one successful breach a year

46%
Canadian organizations are not confident in their ability to defend against attacks

47%
Canadian organizations had sensitive data stolen

- One-in-five breaches was classified as "high-impact", where sensitive customer or employee information was exposed.
- 36 percent of respondents are not confident in their company's ability to respond to security breaches.
- A majority of respondents do not train employees to identify attacks, such as phishing scams, or to update software with the latest security measures.
- Almost three-quarters of respondents don't comprehensively analyze how third-party relationships affect their overall cyber security planning.

We see this first hand. Because of what we do, we get the calls when business owners get hit. When data is stolen or corrupted and they face a real crisis in their business. At that point, businesses will pay anything to get their data back, to get their business back on track. Sometimes, we can help them. Sometimes nobody can. But in almost every case, the damage could have been prevented or minimized with a relatively small effort and expense up front.

THE BUSINESS CASE FOR CYBER SECURITY

There are three major areas where your company can feel the impact of lax cyber security policies and processes.

1. New Legislation and Regulation — Rules and Penalties

In November of 2018, the federal government released new regulations that have an impact on all businesses — regardless of size. This new set of rules requires you to record and report security breaches. You must keep a record of security issues as specified by the government for at least two years — maybe more. If the breach could result in what the government deems to be harm to a person — ***you are required to notify the government and anyone affected***.

There are real penalties for failing to meet these requirements.

The government doesn't take you to court — they level what are called administrative penalties. These penalties can be as much as 100,000 dollars for each person affected. These are what is referred to as "administrative penalties". You are not presumed innocent til proven guilty.

The size of your company and even your ability to pay is irrelevant. The same rules apply if you have two employees or twenty thousand. And if you look at the history of government regulations in recent years, they will go after companies big or small. They don't care. Once you hit their list, you're on the hook.

So in realistic terms how much can you be fined? The regulations are new and we haven't seen any fines yet. But if we take what the government has done in other regulations like the anti-spam legislation (CASL) we can see that some companies were fined hundreds of thousands of dollars or even in one case, over a million dollars. More realistically, these fines have ranged between twenty and eighty thousand dollars which for many businesses is still significant.

Add that to the reputation and possible customer loss when you have to notify your best customers that their data has been breached.

Are you personally responsible? In many cases your company is accountable. We are not lawyers,

but we have read credible pieces by law firms that indicate there are instances where even directors of a company may be held accountable for actions or their inactions.

What do you have to do to comply?

What do you have to record and disclose? Canada's new privacy regulations require that you must keep records of ANY breach of your security for up to two years. And you must provide the following information to the commissioner and those affected if there can be any risk of harm from its a breach of security.

This is an excerpt from the government compliance advice which says you must provide:

- a description of the circumstances of the breach;
- the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extent that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- contact information that the affected individual can use to obtain further information about the breach.

To comply with the requirements of the regulations (above) you need to have policies, processes and training in place that meets at least a minimum standard of protection. You have to detect and record any breaches of security — wherever they occur.

2. Lost Reputation and Lost Customers — More Than The Money

Just imagine having to write to all or your clients to explain to them that they might be victims of a security issue. This is going to have an impact. Would you know what you have to do? Would you know when you have to notify them?If not, you have a real risk and open yourself to government penalties and potentially legal action. Again, we're not lawyers so we can't tell you how well you might fare in a legal action. All we know is what we've been told. A reasonable defence could be made if you've done what is commercially reasonable best practices. But even if you win the legal battle, you could still lose a customer.

With all of the publicity about security breaches, customers are much more wary. If they suspect or hear about a problem, or see that your site is unavailable, they will move somewhere else in a heartbeat.

“With all of the publicity about security breaches, customers are much more wary. If they suspect or hear about a problem, or see that your site is unavailable, they will move somewhere else in a heartbeat.

Even if customers miss the outward signs there are sites and services that will report whether your company has been breached. A new threat from hackers is to get you to pay a ransom so they don't post your customer info to the internet. But even without that, your customers can find records of breaches online on a number of sites and services. And of course, as we mentioned, under current regulations, **you have to record all breaches and if harm is possible, report them to your affected customers**. No matter what — if an incident happens it will get out. In a world of social media, it's hard to keep a secret.

If your company deals on a business to business basis, the story gets worse. More and more businesses are requiring that you certify that you can protect their data before they will do business with you. They need this to comply with regulations and to protect themselves. When you get these contracts, read them carefully and see what you are accountable for.

Even if you are willing to sign anything — will you be able to share the evidence — policies, procedures and security review? Most companies would stumble. Anyway you stack it, failure to have a real cyber security program could lose customers or that big sale you worked so hard to get.

The impact of cyber security on your sales and customer retention is clear — a recent study conducted by the Canadian Internet Registration Association (CIRA) stated that

85 per cent of customers felt businesses should do more to protect their data and 75 per cent said they wouldn't buy from a company who they felt couldn't protect their data.

SO WHAT'S HOLDING YOU BACK?

In our experience, companies that have disasters fall into two groups. The first has a false sense of security. They think that they have more protection than they have. They think their cloud service will protection them. Or that anti-virus will keep them safe. There's a brutal reality here. Most of what you think will work, will not really save you.

The second thinks it's hopeless to try to keep up with all the craziness out there. New threats emerge every week. How on earth could you keep up?

It's compounded by informationoverload.Even if companies want to do something, where do you start? Everyone claims to have a "silver bullet". They can't all be right. And everyone wants to sell you something. What information can you trust?

We understand. Here's the straight goods. First, it's not as difficult as you think. Second, although you can't stop every risk, you can vastly reduce the chance of an issue and the impact when a security issue happens.

Notice that we didn't say if. We are not exagerating when we say everybody gets hacked or has a security breach or failure. Even the smallest businesses find themselves victims.

According to the independent authorities, in Canada, 70 percent of cyber attacks happen to companies with less than 100 employees.

Today, hacking is a growth business. Malware is everywhere. And even a piece of hardware fails eventually. So it's not IF, it's WHEN you have an impact.

WHAT KIND OF THREATS ARE OUT THERE?

There are a wide range of possible threats and they change rapidly based on the creativity of the attackers. But the top 5 according to a Canadian Internet Registry Authority (CIRA) study were:

- **Viruses and other malware:** software created with the sole purpose of spreading from computer to computer. The main intent is simply destructive vandalism.
- **Phishing:** emails designed to trick you into giving away passwords and login details or to extract other information which is then sold or used to defraud or hack your organization — or both. Even when a small business is attacked, the amount of research and planning that can go into these is intense. These highly targeted events are called "Spear Phishing". Phishing is used as the start of many types of attacks. Once the hackers have user credentials or information or both, they leverage these to mount other attacks.'
- **Trojans:** malicious software that is designed to hide on computers and do damage or steal data in stealth mode.
- **Spyware:** spies on you or your activity and reports it back to a hacker. It could be pictures, it could be keystrokes.
- **Ransomware:** will encrypt the data on your computers and hold it hostage until you pay a ransom, at which point you may or may not get back your data. Until last year, this was the biggest growth area in hacking — and although it's no longer growing at double digit rates, it's still in the top five of risk areas.

These are only the top five. There's an amazing amount of creativity out there with combinations of these threats or new threats emerging all of the time.

KIND OF THREATS

Viruses and other malware | Trojans | Phishing | Spyware | Ransomware

NEW AND CREATIVE THREATS

One recent "Spear Phishing" attack used social media to know when the President or other key person was occupied. Maybe they were on their way to the airport, maybe at a kids soccer game. That's when the thieves would send a note about a new supplier that had to be paid, complete with an authentic looking invoice.

Another growing problem steals computer resources from laptops and servers. In the "olden days" — a few years ago, hackers would use your computers to launch attacks or to hide their identity. Either way, your company was an unwitting accomplice. This not only steals resources but it also exposes you to investigation and blacklisting from important services.

Lately, stolen computer resources are used in so-called "currency mining". Bitcoin and other resource in intense cyber-currencies require vast amounts of processing power and reward those who provide that processing. This has generated a cottage industry based on stealing computer cycles from a wide range of devices.

In the world of cloud computing where you pay for what you use, you can be defrauded of a large amounts of money for resources that are simply stolen. Don't think that you will be absolved because you were illegally attacked — if you read your contracts, you will often be presumed guilty of not doing enough to prevent the attacks. It's called "shared responsibility" in many cloud service contracts. Few people have read that before clicking "accept".

HOW DO WE REALISTICALLY UNDERSTAND OUR RISK?

There's a lot happening out there. It changes daily. So it's quite a realistic for businesses to ask, "how do we understand our risk and prioritize what actions we take?" It's a great question.

The short answer is this. Each business is different. Each has different risks and priorities. The best way to get a clear handle on what your level of risk is would be is to do an assessment of the risks, the impacts, and the probabilities and the ways you can remediate the risk. There are professionals who can do this quite quickly and come back with a realistic look at where your risks are and what you need to do.

How much you need to do depends on a number of factors. Some businesses could do a relatively quick review. Others may have complex issues or customers who want another level of detail.

Only you can decide how much protection you need. A good analysis will help you understand and make appropriate decisions based on your business and your risk tolerance.

To get you started, we've taken a very simple approach and created a two page assessment that you can do for yourself in a very short time — maybe 20 minutes or less (and that's if you have to call someone for a few answers).

Try it out and see what you think. It may reveal problems, give you something to think about or maybe give you some level of comfort about your current situation. It's free, it doesn't cost anything and nobody will collect your data.

You can download the assessment at
https://padv.ca/simplesecurityassessment

If after doing that self assessment, you think it's wise to look a little further here's what you might think about:

SO WHAT DO YOU NEED TO DO?

Every business, regardless of size or industry has to take security seriously. That doesn't mean you have to spend a gazillion dollars or buy everything that some security vendor or consultant wants to sell you.

The first big step is a proper assessment. The self assessment is a good start but you need a little more detail of what they issues and risks are before you develop your Security and Business Resumption Plan.

BUSINESS RESUMPTION PLAN

Every business needs a plan. Not reams of paper or huge amounts of text. You need a smart and simple 6 step plan that will:

1. Identify the data that forms your key "assets" that you need to protect.
2. In light of what you need to protect, do a full assessment of your risks and threats
3. Develop a Security Strategy with clear action items prioritized based on risks and greatest areas of impact.
4. Implement some basic technical steps to vastly reduce your exposure
5. Implement basic policies and procedures to:
   - Comply with government and other regulations
   - Educate your employees on how to detect and prevent attacks.
6. Create a plan for Business Resumption — how to mitigate and recover from an attack.

It is really that straightforward. Although there are technical issues which you should address, having strong security is as much about culture and behaviour as it is about technology. You can't fix everything at once, but you can reduce your risks and increase your ability to recover from an incident.

Here's some things to think about:

- **A data inventory:** Most of your risks are in direct relationship to your data. If it's destroyed, compromised or otherwise affected, your business feels the impact. You need to understand where your data is, and most important, what is the most critical data — your "crown jewels". That will drive all of your subsequent actions and it will ensure that every action you take is focused and practical.
- **An assessment of your risks and potential areas of vulnerability:** Once you know what you are protecting you need to look at all of the places where you are vulnerable based on your data and the threats that are out there.
- **Technical steps:** There are key things that everyone can do to reduce their exposure dramatically. For example, keep your software up to date. This is more than just updating your antivirus, although you should do that regularly. But if you keep your other software up to date you will find that you are automatically protected against threats. Software companies regularly find vulnerabilities and update their software. In the process, the announcement of those updates lets hackers know where the vulnerabilties are. So if you don't update, you are an easy target. Just scan and attack. Most companies don't do these updates, which is why the most prevalent attacks exploit weaknesses that have been known for years. A simple update would fix it.
- **Processes and Procedures:** Even a small investment in changing employee behaviours and and ensuring a few basic procedures can vastly reduce risk. It can also ensure that you comply with government regulations. It's

too late to debate what you should do once you've been attacked. The time to think about it is before it happens. The good news is that there's a lot of great material out there. You don't have to reinvent the wheel. Just take what exists and update it to fit your needs. The trick is not just having the policies and procedures — its making sure your employees use them.

- **Training:** Even simple training on passwords and how not to be fooled by phishing and other exploits has been proven to reduce risks enormously. Those who do regular training fair better still. It's a minor investment for a major payback.
- **Backups:** Most attacks involve loss of data. Whether its stolen, corrupted or just accidentally deleted, if you have a recent backup, you can recover. Given this, you would think that all companies would have backups and that they'd test them regularly. Unfortunately, as all too many discover, when the times comes to restore data, they cannot do it. Backups get missed, they are not current enough, they take too long to restore or they were never tested and just don't work. It can literally cost pennies per processing hour to have a viable, functioning backup for key systems.
- **A business resumption plan:** How you respond to a breach, a disaster or even just an interruption can have a big impact on your business. It's really just finding the answers to the key questions that you'll need to answer. What would you do if this happened in the middle of the night? Who would you reach? How do you contact them? Who makes decisions? Who gets notified? Where would you get the equipment or skills to resume business? Every business needs a plan and a way to know what will happen, who will make the decisions and what you will do to get up and running quickly.

YOU DON'T HAVE TO DO THIS YOURSELF

Companies want to do the right thing, but they have to balance security with what they can afford and what is realistic for their business. Large companies can have full time staff that handle all of the complexities of security and business resumption. Yet even these companies find it difficult to attract and retain good people.

You do not have to hire a full time staff for security. You do not have to spend a fortune. You can buy "security as a service" just like you buy software. Our firm offers what we call a "virtual Chief Information Security Office". It provides everything you need to get started and to keep you current with new developments. We provide:

- **Data Analysis and Risk Assessment:** Our certified and trained security professionals will do a rapid assessment of your risks and potential threats as they relate to your business. We have taken standards, regulations and best practices and put them into a framework which we adapt to your business. Our analysis and recommendation will explain to you in real terms what your risks are in terms of your business and our practical set of recommendations that will allow you to make real business decisions on the level of risk and cost that is appropriate for you.
- **Policies, procedures and training:** A huge amount of risk is removed by having appropriate policies and training in place. We have processes and procedures that can save you time an effort by adapting what others have developed as best practices to your own circumstances. No sense in reinventing the wheel. In addition to helping you draft these policies and procedures we'll help you focus on how to leverage them to really reduce your risks. It could be things like strong passwords, training on major risks and ways to avoid them or simply keeping you up to date with new developments.
- **Backups and testing to prevent data loss:** Most companies think this is working, until they have to use a backup and find out that it's not there. Or they find out that their cloud provider won't rescue them from an accidental deletion. Or that their backups don't allow you to recover because something is missing. Or worse, backups

don't work at all. Or they have someone hold their data for ransom and can't recover. Each of these risks could be vastly reduced with an effective solution and regular testing.

- **Regular software updates:** Hackers today often exploit weaknesses in software where the software provider has patched the problem. In fact, many hackers use the software patches to "reverse engineer" their attacks. The most popular attacks exploit weaknesses that have been known for years. But companies don't patch and update because they don't have the time or resources. It's another simple way to vastly reduce risk.
- **An up to date business resumption plan:** If you have access to your data and a good recovery plan, you can be back up and running in a very short period of time. If you have a plan and a way to execute it. In past years, this could be expensive, but with some of the options that are available today, there is no reason not to have a recovery plan that will get you up and running before your business in severely affected.

LET US HELP

Our job — our passion — is to take care of technology so that you can take care of business. We'd love to help you prevent issues that can have an impact. We're also here to help you if you get hit. No judgement. No buzzwords. Just straight talk, expertise and a dedication to your success. Let us be your "Performance Advantage".

Take our free assessment. Give us a call. Or when our representative calls, take a few minutes to find out how our practical approach can help you.

CONTACT US

Performance Advantage
web: www.performanceadvantage.ca
email: hello@padv.ca
phone: 1-888-543-7810