10 steps to an effective **cybersecurity program**

For small and medium-sized businesses

A 10-step cybersecurity strategy that small and medium-sized businesses can use to minimize their cyber risks.

ROGERS cybersecure catalyst

Contents

3
It’s time to take control of your cybersecurity

4
Phishing attacks

5
Ransomware

6
Business email compromise

7
Weak passwords

8
Insider threats

9
Summary

10
Step 1:
Asset inventory — know what you have

12
Step 2:
Passwords

14
Step 3:
Access control

16
Step 4:
Secure the cloud

18
Step 5:
Back it up

20
Step 6:
Network security

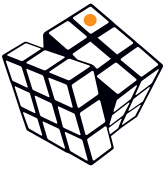
22
Step 7:
Plan for the worst

24
Step 8:
Education is key

26
Step 9:
Tie it all together with policies

28
Step 10:
Select the right vendors

28
Going forward



28
Glossary

It's time to take control of your cybersecurity

Cybersecurity is one of the most urgent and pressing concerns of business owners, big and small. Leaders from C-Suite to boards of directors are starting to recognize the importance of embracing a cybersecure culture within their organizations. Every week, new stories emerge about data breaches affecting customer records, payment card data and loss of trade secrets.

Conventional wisdom has shifted from a mindset of IF we are hacked to WHEN

Attacks are growing both in sophistication and their nefarious intent. Such attacks are becoming so common that the conventional wisdom has shifted from a mindset of IF we are hacked to WHEN and how badly will we be affected. As a result, the best prepared companies are shifting their cybersecurity strategies from focusing on outright prevention to implementing techniques to limit the damage, recover quickly once a breach has been confirmed and minimize the possibilities of a breach occurring again.

This guide is going to

Introduce you to the threats facing startups and small businesses, and the even BIGGER OPPORTUNITY they present

Help you turn cyber risk into competitive advantage

Guide you to think about how to build an effective cybersecurity program that will scale as your business does

Let's begin by looking at the

top 5 cyber threats that startups and small businesses face

1. Phishing attacks

The biggest, most damaging and most widespread threats facing startups and small businesses are phishing attacks.

Phishing accounts for *90%* of all breaches that organizations face - they've grown *65%* over the last year and account for over *$12 billion* in business losses.

Phishing attacks refer to an attacker pretending to be a trusted contact, and enticing a user to click a malicious link, downloading a malicious file, or grant access to sensitive information, account details or credentials.

Part of what makes phishing attacks so damaging is that they're difficult to combat. They use social engineering to target humans within a business, rather than targeting technology weaknesses.

Phishing attacks have grown in sophistication, with attackers becoming more convincing as they pretend to be legitimate connections. As a result, getting a user to click a link from what looks to be from a trusted source, exposes an organization to other potential attacks.

There are technology solutions that can be put in place that can help prevent phishing emails from reaching yours and your team's inboxes. Certain technologies and applications can even allow users to report phishing emails and then allow designated admins to delete them from inboxes. But these can't be the sole source of protection.

The most effective layer of security to protect emails from phishing attacks is Security Awareness Training.

These solutions allow you to protect your company through training and assessment of employees on how to spot phishing attacks.

ALL YOUR FILES HAVE BEEN ENCRYPTED
Computer files have been encrypted. But, don't worry! I haven't
5000 USD in Bitcoins to my Bitcoin
Address to get your files back.
files will be deleted. After 72
hours all that are left will be deleted! We will format your hard-drive when
you restart the Computer! The Timer starts now! - BadActors ;)
TIME LEFT: 71 : 59 : 47
Send 5000 USD worth of BitCoins here:
14k81d3PHfB8A3GJAGa1wmbRdE7x7fgby8

2. Ransomware

Ransomware is one of the most common cyber-attacks, hitting thousands of businesses every year.

Ransomware is generally the second step in attack after the phish and having an employee click on a link. Attackers are continually testing their ransomware software against antivirus engines to prevent detection. So even if you have antivirus software installed, there is a good chance that it will not detect the ransomware.

Ransomware is one of the most lucrative forms of attacks and its popularity within the attackers circles is growing. Ransomware involves getting access to an organization's data, systems, networks, etc and encrypting company data so that it cannot be used or accessed. Attackers then force the company to pay a ransom to unlock the data, leaving businesses with a very tough choice – to pay the ransom and potentially lose huge sums of money or cripple their services with a loss of data and potentially rendering their systems unusable for a period of time.

Startups and small businesses are especially at risk from these types of attack.

In 2018, 71% of ransomware attacks targeted small businesses, with an average ransom demand of $116,000.

Attackers know that small businesses are much more likely to pay the ransom, as their infrastructure may not always allow for them to combat such attacks. Small businesses also often don't have the mechanisms for data recovery because their data may not be backed up, significantly reducing their ability to get back up and running.

Businesses must have an effective backup process in place.

An effective backup process is to have multiple backups to ensure the integrity and security of your corporate data. With this type of approach, commonly called Belt & Suspenders, if one fails in the face of an attack, you can still restore your data and become operational sooner.

3. Business email compromise

Business Email Compromise (BEC) is another concerning trend that can result in defrauding of companies by millions of dollars.

As with the above two threats, it involves social engineering but instead of having employees clicking malicious links, it has cybercriminals performing fraudulent money transfers or manipulating employees into transferring money to their account.

From creating fake invoices to taking over the email accounts of CEO's hackers can use business email compromise attacks to trick and manipulate unsuspecting employees and executives, all at a high cost to unsuspecting businesses.

The concept behind the attacks is relatively simple: use email to trick companies into wiring money where it isn't supposed to go – the attacker's account.

Business email compromise scams tend to be aimed at senior executives or those who oversee transferring of funds.

Typically, the fraudster has done their research on the company by following press releases, reviewing the company website and social media, and employee social media accounts. This provides attackers with information on an organization's current projects, and the individuals involved, an email can then be crafted with sensitive information and, manipulates them into transferring funds to attackers.

Another technique involves either taking over the email account of a vendor's employee. Attackers can then use this position to send out invoices to their target company with a sense of urgency such as taking the company to collections or to court if the outstanding balance isn't paid. They will then follow up with the target company and come up with a ruse to get the target company to change the account number from the vendor to their own account. The target then transfers the funds to the account, thinking that its vendor has simply updated its account details. Instead, the payment is sent directly into the attacker's hands.

4. Weak passwords

Another threat facing startups and small businesses is employees using weak or easily guessed passwords, or reusing passwords for multiple accounts.

Many businesses use multiple cloud based services, that require different accounts. These services can often contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts can cause this data to become compromised.

Passwords are sold on the dark web, and attackers purchase them to use them against corporate xaccounts and for social engineering attacks. Never use a password for a personal account on a corporate account, no matter how strong it is.

Have a look at the Worst Passwords for 2019 from Splashdata - it is evident that weak passwords are still a risk in today's hyper connected business landscape:

1. 123456 (same as 2018)
2. 123456789
3. Qwerty
4. Password (this was #2 in 2018)
5. 1234567
6. 12345678
7. 12345
8. Iloveyou
9. 111111
10. 123123

Cybercriminals are armed with the latest technology and can launch what are called brute force attacks. They use automated programs that can guess billions of password combinations per second. In fact, using commercially available computer components, current password cracking benchmarks show that the minimum 8-character password, no matter how complex can be cracked in less than 2.5 hours.

5. Insider threats

Another major threat facing startups and small businesses is the insider threat.

An insider threat is defined as the risk to an organization caused by the actions of employees, former employees, business contractors or associates, either knowingly or unknowingly. These actors have access or can gain access to critical data about your company, products or intellectual property, and can use such information to cause your organization harm or threaten its operations and success. This can be a result of greed or malice, a desire to cause your organization harm or simply through carelessness.

The Verizon Data Breach Investigation reports that the percentage of companies that suffered from malicious insiders rose from 25% in 2016 to 34% in 2018.

This is a growing problem and can put employees and customers at risk, or cause the company financial damage. Within startups and small business, insider threats are growing as more employees have access to multiple accounts that hold more data that is sensitive. Research has found that ***62%*** of employees have reported having access to accounts that they probably shouldn't have had access to in the first place.

Resilience

Summary

The threat landscape for small and medium businesses continues to grow as does the sophistication and frequency of these attacks.

This makes SMB's more vulnerable than ever, due to the level of damage these attackers can cause, be it financial or reputational.

The best way for startups and small businesses to protect against these threats is to have a comprehensive set of security best practices in place and ensure that all employees are familiar with such practices.

Now that you're familiar with the most prevalent threats, we'll introduce you to the...

10-steps

that can help you build towards an effective cybersecurity program

Step 1: Asset inventory — know what you have

Asset inventory is the foundation of cybersecurity.

Know what hardware and software you are using, in order to effectively protect it.hardware and software you are using, how can you effectively protect it?

What should be on your inventory?

You should track all technology (computers, printers, network devices such as routers, WiFi extenders, switches and mobile devices), software applications and data that reside on the assets.

What should you track?

Once you have performed an inventory of technology assets, you should identify and track certain key pieces of information associated with those assets:

- Unique identifiers for the asset (i.e. machine name, serial number)
- Owners and/or users the asset
- The geographic location of the asset
- The criticality of the asset i.e. how important it is to your business (i.e. low, medium, high)
- The business process function the asset supports i.e where it falls within your workflow and the role it plays
- The version of the operating system associated with that asset
- Any applicable software versions or updates that have been performed
- The amount and capacity of the software being licensed (i.e. how many seats do you have)

Having this information at your fingertips will give you a wealth of information to make important security and privacy decisions. Your inventory should also help drive your patching program. Patching is a critical exercise to ensure you are running the latest and most secure versions of the operating systems and applications.

Step 2: Passwords

Passwords can often be the weakest link in the cybersecurity chain.

Passwords have become an increasingly unreliable way of securing data and the real problem is that effective passwords are difficult to remember.

It may not be reasonable for people to keep track of a long, complex password for every account they have. This issue is known as "password fatigue" and it often leads people to reuse the same password across multiple accounts, which is one of the worst security mistakes to make.

To ensure the effective use of passwords, try and follow the below outlined best practices that will ensure passwords are working for you and not against you.

Password Best Practices

••••••••••••••••••••

- ✓ Create passwords with a minimum 12-16 characters
- ✓ Build complexity by using a combination of words, numbers,special characters, symbols, and upper and lower case letters.
- ✓ Choose passwords that are easy for you to remember but not predictable and harder to guess for others.
- ✓ Change your passwords at least once every three months
- ✓ Use a different password for every application and website
- ✓ Use a password manager
- ✓ Enable Two-factor authentication (2FA) where available
- ✗ Do not use personal details that a lot people know about you such as your birthday or names of friends, family and pets.
- ✗ Avoid using common dictionary words or proper nouns
- ✗ Never share your passwords with anyone, even if you trust them

Step 3: Access control

Access control is a process that helps manage and regulate who or what can view or use applications and data in your organization, and what level of access to grant them.

It is a fundamental concept in security that helps minimize risk to your business by limiting access to data, workflows and functionality, to those that require it to perform their job function.

There are two types of access control: physical and logical.

Physical access control limits access to physical infrastructure such as buildings, rooms or physical hardware. Logical access controls limits connections to computer networks, system files and data.

Access control systems perform identification authentication and authorization of users by evaluating required credentials that can include access card details, log in details, passwords or personal identification numbers (PINS).

Most startups and small businesses share the common trait of moving at a quick pace and need to be nimble in their decision making. They are often expanding reach, moving locations developing products, hiring new employees and implementing new systems all in parallel. This rapid pace of change and growth can often overlook the need for a planned approach to access control, instead leaning towards providing as much access as possible to whoever needs it. This is a mistake.

Without having a method of controlling what level of access is granted to which individual, systems and data end up being vulnerable and exposed to attacks.

What steps to take

By implementing Access Control early, you don't need to sacrifice speed for security. Following what is called a Zero Trust or Principle of Least Privilege principle, you can protect systems, valuable intellectual property and valuable time by minimizing the risk of breaches.

Benefits of implementing a Least Privilege principle:

- Avoiding malware propagation
- Limiting entrances for malicious actors
- Improving data classification
- Complying with regulatory requirements
- Reduce insider threats

Implementing Microsoft Active Directory, Microsoft Office 365 for Business or Google G Suite for Business are great ways to implement access control. Zero trust principles are often built into such systems and you can use their frameworks to help kick start your organization's access management process.

Step 4:
Secure the cloud

Let's start with a quick primer on the cloud.

The "cloud" is a server or a network of servers that are accessed over the internet to run software or services (such as software applications, storage and processing power) remotely instead of locally. Essentially it allows you to use the infrastructure provided by others instead of having to invest in your own.

There are three (3) types of cloud services used by businesses:

Public Cloud is the most common, when people speak about the cloud. The computer resources (like servers and storage) are owned and operated by a third-party service provider and delivered over the internet. Applications such as Microsoft Office 365, Google G Suite, Quickbooks and Shopify are public cloud services.

Private Cloud consists of computer resources used exclusively by one business or organization. The private cloud can be physically located at your organization's site or hosted by a third-party service provider in their data centre and accessed over a private network.

Hybrid Cloud is a combination of Public and Private clouds. Data and applications can move between public and private clouds for flexibility. A business case may choose to host their high-volume applications such as email on the public cloud and then use the private cloud for more sensitive, business critical applications such as financials.

Cloud technology has brought new opportunities for startups and small businesses to compete on a global scale. Thanks to innovative products that provide storage, software, and infrastructure through the cloud, businesses can minimize their IT expenses. With these benefits, come many of the same risks that businesses face with their own networks. Some of the top risks include:

- Misconfiguration. Cloud applications are often deployed with the default security configurations, which in most cases are configured to be user-friendly rather that security-friendly or risk focused.
- Compromised credentials. If a hacker gets the administrator user credentials, the scope of nefarious activities can range from changing user passwords – denying access to you and your users - to being able to delete all your data.
- Weak access management. Some cloud applications do not allow you to implement a principle of least privilege. In essence your users have the keys to the castle.
- Data jurisdiction. When you move data to the public cloud, you lose visibility into where your data is actually stored. This may pose an issue if you're adhering to regulations like GDPR, HIPAA, PIPEDA and PCI DSS.

It is best to think of a cloud application as an extension of the business network. Many of the steps in this document such as strong passwords, multi-factor authentication, access control and data backup are essential steps to implement with cloud applications as well.

That is why it is important that you do your due diligence before selecting a cloud provider. Here are some questions that may help kickstart your process to finding the right cloud solution provider:

1. Where is my data stored? Where are your data centers located?
2. How secure is your cloud and what are your security best practices?
3. How do I access my data on your cloud? How does it integrate into my organization's workflow?
4. How do you handle regulatory compliance? (PCI-DSS, PIPEDA, GDPR, etc)

Step 5: Back it up

While many companies deal with confidential data on a daily basis, not all understand how to properly take care of that data. Many small business owners are unaware of the risks that data loss poses to their business.

When that data is confidential, such as a customer's personal data and credit cards, the risks are even higher.

Many SMBs believe that any loss, either from security breach or lack of disaster recovery, would not seriously hurt the business.

Remember, a loss is not always immediately quantifiable and can come in many forms such as, the loss of customer trust, reputational damage, or even a lack of compliance to industry regulations.

Improving data security starts with ensuring files are recoverable should loss occur for any reason. Following a frequent and effective backup process is a simple yet effective way of ensuring that your data is recoverable from its closest point in time.

Steps to improve your data security through backups include:

1. **Multiple Backups.** The 3-2-1 backup rule is easy to remember. It is good practice to have 3 separate backups – two different offsite copies (in the cloud and other media) and one onsite. All 3 should be encrypted to ensure the confidentiality and integrity of your data.
2. **Air gapping.** At any given time, at least one of your backups is offline or disconnected from computers and cannot be accessed. If the backup has no connection it cannot be hacked or corrupted.
3. **Testing.** This step is the hardest and most critical. Testing can range from restoring random files from your backups to performing an actual recovery to an alternate server, location, etc. Testing your backups ensures you have the ability to recover your data.

Step 6:
Network security

Network security is much more than the satisfaction brought about the blinking lights of the physical network. The many layers of Network Security is the core of its complexity.

Every organization that delivers services that customers and employees demand, must protect its network. Ultimately it protects your reputation.

1. **The first layer of defense for your network is the firewall.** The firewall provides a barrier between your data and the internet (and the cybercriminals) to prevent unauthorized access. A firewall can be implemented as a hardware or a software solution, or a combination of the two. A wireless router/firewall intended for home use quite often doesn't have the functionality that a business requires to implement proper network security. Look into solutions that are meant for small and medium sized businesses. A good place to start may be your local Internet Service Provider that offers business grade solutions.
2. **Install anti-malware software.** As discussed above, malware can be damaging to businesses and it is often a simple but effective technique for attackers to use. It's easy to assume that your employees know to never open phishing emails but with the right education and the use of an anti-malware software installed on all devices on your network you can take steps towards protecting your network's security.
3. **Plan for mobile devices and users.** Most startups and small businesses allow employees to use their own laptops and mobile devices. This practice is called Bring Your Own Device (BYOD). While it seems attractive from a capital budget perspective, it adds security risk to your organization. Your employee's devices could become a target and if they aren't secure they could be the attacker's way into your network and your data. One important step towards securing your employee's devices is to ensure the devices run anti-malware software, have automatic updates turned on and require secure passwords. Build a plan for your organization that outlines these steps to ensure existing and new employees are following best practices.
4. **Vulnerability management.** Every network has vulnerabilities, and attackers take advantage of the vulnerabilities to gain access. A great analogy is your body. You should go to the doctor to get a checkup every year. It helps you stay on top of the health of your body. The same goes for your network. You should have a vulnerability assessment completed at least once a year to assess the general health of your network to look for potential problems that could harm your company.

Step 7: Plan for the worst

"Hope for the best, but plan for the worst", there is no denying what the phrase means and the value it holds when it comes to your organization's cybersecurity. You should have a positive outlook, but make sure you are ready for disaster. This step is all about planning for what could be and not just what is.

1. Business Continuity

The Business Continuity Plan (BCP) is essential to effective risk management. A well-designed plan will help you minimize the risk that an emergency poses to your employees, clients and suppliers, and help ensure the continuity of your business operations during a crisis. Your BCP should start include documentation of critical business functions and how you would manage them in the time of an attack without reliance on technology.

2. Disaster Recovery

The plan should start with outlining your data sets and the disasters you want to protect against. Define your recovery priorities and identify them in order of what's most important. The detail should entail what data is being backed up, and how quickly you need to recover it to resume business functions.

Also make sure to update your disaster recovery plan as your organization scales and adopts new systems and resources.

3. Cyber Incident Response Plan

A Cyber Incident Response Plan provides a roadmap to follow when a breach is discovered. It is a time saving and stress reducing tool. Once your plan is in place, you won't have to waste time and energy deciding what to do when a breach occurs. Your plan should identify the different team members, vendors and technology providers, on your crisis response team. It should set clear expectations of each team member and how the need to respond. And you should also develop a plan for crisis communications to internal and external stakeholders including your customers.

4. Cyber Insurance Coverage

Cyber insurance is a simple and effective way to ensure you are covered in the event of a cyber breach and is designed to help you deal with the financial ramifications associated with it. A cyber insurance policy addresses the following issues:

4.1 Risk management services

4.2 Data restoration costs

4.3 Liability coverage for legal fees, and coverage for the cost of paying judgements, if you lose a court case stemming from a data breach.

There are several cyber insurance providers that offer this service, make sure to find one that can offer you a solution that works best for your industry and type of business.

Like all plans, the above require you to periodically test your plans, your people and your processes and continue to improve upon them.

Step 8: Education is key

Your people are your strongest defense. Building cybersecurity awareness in a startup or small business reduces the risk of a security breach and helps protect you from attackers looking to cause your business harm. The goal of an awareness program is to raise awareness of cybersecurity risks and best practices with employees so that they make better decisions and protect your business.

The threat landscape is constantly changing with new and more sophisticated techniques being used by cyber criminals. As a startup or small business you need to keep up with the risks that they pose to your business. Some of the risk come from your ability to provide attackers access to a larger system. Large organizations often have a range of vendors and service providers, many of them being startups and small businesses. If you remember the hack that the large American retailer experienced, cyber criminals gained access into Target's systems through access to an HVAC company that did business with Target. As a result of breaches like this, organizations now run third party risk assessments on their vendors. One of the requirements on most assessments is cybersecurity training for employees.

The 3 Steps to Building a Cyber Awareness Program

1. Define your why

Why is cybersecurity and cyber awareness vital for your business? Ask yourself what will happen to you and your business if there's a breach. Will you lose clients? Will you lose revenue?

2. Develop your plan

Remember that cyber awareness is a continuous process; it is not an event. So start with sharing why cyber awareness is important to your business with your leadership team and how it impacts them in their roles. Awareness is really about teaching everyone in the organization about the risks and best practices to identify and avoid those risks.

3. Deployment and Execution

There are multiple ways to deploy the program - some companies incorporate it into their weekly team meetings. Others email employees weekly on important topics or risks. The goal is to create a culture of awareness within your company.

Cybersecurity awareness not only empowers employees to protect an organization from cyber threats but it also helps you assure your stakeholders that you are thinking about the integrity of your systems and business operations. You can grow your business by differentiating yourself through cyber awareness. Showing customers and employees the importance, you place on their information can sometimes be the differentiator that gives you access to new business opportunities.

Step 9: Tie it all together with policies

Put simply, a cybersecurity policy is a statement, or a collection of statements, designed to guide employees' behavior regarding the security of company data, assets, etc.

These policies define the who, what and why regarding the desired behavior, and play an important role in an organization's overall security posture.

The goal when developing cybersecurity policies is to provide relevant direction while identifying the value it brings to the individuals within an organization.

Some tips for developing cybersecurity policies:

1. **Understand the role of the policies.** The policies protect your organization's critical information by clearly outlining employee responsibilities regarding what information needs to be safeguarded and why.

2. **Ensure your policies are enforceable.** A policy is only as good as your ability and motivation to enforce it. It is important that everyone from the CEO to the most junior employee complies with the policies and often leadership has to set the example. If management doesn't comply with the security policies and the consequences of non-compliance with the policy is not enforced, employees can either dismiss the use of such policies or mistrust and apathy toward such policies can plague your organization.

3. **Make your policies brief and concise.** Supporting procedures can fill in the how and when of your policies. Each policy should address a specific topic (password security, acceptable use, access control, cloud computing, etc.); it will make things easier to manage and maintain. When employees understand security policies, it will be easier for them to comply. Remember, complexity is the enemy of security when it comes to your employees. Address specific topics, provide clear direction and lines of accountability, and build a process that works for your team and organization.

4. **Keep the policies current.** Because cybersecurity is constantly changing, security policies need to be updated frequently. At a minimum, security policies should be reviewed yearly and updated as needed. When updated, it is good practice to disseminate that information to your employees and have them acknowledge the changes.

Startups and small businesses often have informal, and undocumented policies and procedures; cybersecurity is one area where it is essential to document your formal protocols.

Step 10: Select the right vendors

No matter what type of business you are in, chances are you will rely on the expertise of a vendor, partner, consultant or other kind of third-party to help you.

A third-party may help you achieve your business goals but they could also introduce a new level of risk to your business.

There are security risks in giving vendors access to your network and data. If the vendor suffers a breach, your company can lose vital business data, the attackers could gain access to your networks and confidential client and employee data can be compromised. This potentially opens you up to fines from privacy laws, lawsuits and a damaged reputation.

It may be impossible to eliminate all vendor risks altogether, but you can contain them a little more through planning.

Here are some steps you can take:

Perform a Vendor Assessment

It is essential to assess the vendor's security standards and best practices to determine if they meet those of your organization. Before entering into an agreement, ask for the vendor's most recent security assessment, vulnerability assessment or penetration test results. This is especially important if the vendor is providing remote support for employees. Vendors that provide these services can be a target of cyber criminals because remote services can provide a back door into many businesses.

Build it in to the Service Level Agreement (SLA)

If your business requires a specific response time or expectation of service, be sure to include it in a service level agreement and that everyone involved is aware of it, especially if the vendor is providing data backup services.

You as a business owner are the custodian of the personal data your clients have entrusted you with. If you suffer a breach due to a vendor's connectivity you can still be held accountable under the applicable privacy laws.

You as a business owner are the custodian of the personal data your clients have entrusted you with. If you suffer a breach due to a vendor's connectivity you can still be held accountable under the applicable privacy laws.

Going Forward

Cybersecurity is a moving target. The cyber criminals get more advanced every day.

In order to protect your data as much as possible, it's essential that you build a culture of security by having every employee make security a top priority and most importantly, that you stay on top of the latest trends for attacks. Your business depends on it.

As a startup or small business, you are in a perfect position to implement these steps while you are small and agile. These steps will serve as a foundation as you grow and bring on more employees. By implementing now, you can save yourself a lot of time and money later.

The most important thing is to get started.

Cybersecurity may appear like an unnecessary cost right now as you are focusing on launching or growing your business, but it is far more costly to recover data, money and your customers' trust.

You will inevitably run into questions along the way. While you know what you need to do, you may not know how to do it. Don't let the questions that arise stop you from taking the next step.

Glossary

Firewall is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of rules. Consumer grade firewalls are intended for home use and prioritize speed over security, business grade firewalls prioritize security and remote access.

General Data Protection Regulation (GDPR) is the European Union's privacy legislation that regulates the collection and use of personal information of individuals who live in the European Union.

Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards. The PCI standard is mandated by the card brands but administered by the Payment Card Industry Standards Council. If you are a merchant of any size accepting credit cards, you must comply.

Personal Information Protection and Electronic Documents Act (PIPEDA) is the Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information during the course of commercial business.

Principle of Least Privilege is the idea that any user, program, or process should have only the bare minimum privileges necessary to perform its function. By adhering to the principle of least privilege reduces the risk of attackers gaining access to critical systems or data by only being able to compromise low-level accounts.

Social Engineering refers to the act of manipulating someone by exploiting them psychologically by tapping into their natural emotional and psychological responses; typically to perform actions that would be harmful to them.

Two-factor Authentication or Multi-factor Authentication is a security system that verifies a user's identity by requiring multiple credentials. Rather than just asking for a username and password, MFA requires additional credentials, such as a code from the user's smartphone to answer a security question, a fingerprint, or facial recognition.

Virtual Private Network (VPN) is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Zero Trust is a network security model, based on a strict identity verification process. The framework dictates that only authenticated and authorized users and devices can access applications and data. In the zero trust model, it is assumed that all users and devices are deemed untrustworthy.

Glossary

Firewall

is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of rules. Consumer grade firewalls are intended for home use and prioritize speed over security, business grade firewalls prioritize security and remote access.

General Data Protection Regulation (GDPR)

is the European Union’s privacy legislation that regulates the collection and use of personal information of individuals who live in the European Union.

Payment Card Industry Data Security Standard (PCI DSS)

is an information security standard for organizations that handle branded credit cards. The PCI standard is mandated by the card brands but administered by the Payment Card Industry Standards Council. If you are a merchant of any size accepting credit cards, you must comply.

Personal Information Protection and Electronic Documents Act (PIPEDA)

is the Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information during the course of commercial business.

Principle of Least Privilege

is the idea that any user, program, or process should have only the bare minimum privileges necessary to perform its function. By adhering to the principle of least privilege reduces the risk of attackers gaining access to critical systems or data by only being able to compromise low-level accounts.

Social Engineering

refers to the act of manipulating someone by exploiting them psychologically by tapping into their natural emotional and psychological responses; typically to perform actions that would be harmful to them.

Two-factor Authentication or Multi-factor Authentication

is a security system that verifies a user's identity by requiring multiple credentials. Rather than just asking for a username and password, MFA requires additional credentials, such as a code from the user's smartphone to answer a security question, a fingerprint, or facial recognition.

Virtual Private Network (VPN)

is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Zero Trust

is a network security model, based on a strict identity verification process. The framework dictates that only authenticated and authorized users and devices can access applications and data. In the zero trust model, it is assumed that all users and devices are deemed untrustworthy.

For more information and our cybersecurity training for small and medium sized businesses, visit our website:

www.cybersecurecatalyst.ca

Ryerson University

ROGERS cybersecure catalyst

ROGERS™