THE COMPLETE GUIDE TO

IT Security for Your Business

COM · PRO
Managed Business Solutions

INTRODUCTION:

Tackling Today's Business Security Challenges

Business practices and IT security risks are constantly evolving.

For IT directors and small business owners, staying on top of the latest threats and best practices can be a challenge.

This may sound daunting, but don't panic!

Fortunately, there are plenty of simple strategies and policies that you can implement to lay a solid foundation of IT security for your organization.

In this guide, we share essential steps you can take to secure your IT infrastructure, workflows, and networks – regardless of whether your team is large or small or whether they are working remotely or at the office.

TABLE OF CONTENTS:

CHAPTER 1

Ten Sobering Business Security Facts

Ten Sobering Business Security Facts

Thinking about all the IT security risks your organization faces can be overwhelming, but you already know that closing your eyes won't make them disappear.

Instead, we believe in looking threats in the eye and taking practical steps to mitigate them. So let's be real and start with these 10 sobering facts:

1. Almost half **(43%)** of cyberattacks target small businesses (source: Accenture)
2. On average, cyberattacks cost a business **$200,000** (source: Hiscox)
3. **46%** of employees admit they transfer files between work and personal computers (source: Lippis Report)
4. **23%** of small and mid-sized businesses don't use endpoint security protections (source: BullGuard)
5. **30%** of small businesses identify phishing as a top threat (source: Verizon)
6. **85%** of managed service providers identify ransomware as the main malware threat to small and mid-sized businesses (source: Datto)
7. **OVER 50%** of small businesses reported compromised credentials in 2019 (source: Verizon)
8. **70%** of small and mid-sized businesses reported lost or stolen employee passwords (source: Ponemon Institute)
9. A hacker attack occurs **EVERY 39 SECONDS** on average (source: University of Maryland)
10. **4.1 BILLION RECORDS** were exposed by data breaches in the first half of 2019 (source: RiskBased)

CHAPTER 2

Working From Home

Work-from-Home IT Security Checklist

These days, more companies than ever have employees working from home. While this has led businesses and workers to become more flexible, it has also expanded the scale and scope of IT security risks.

If you're trying to figure out how to keep your organization safe as more employees work remotely, this checklist provides a good starting point.

COMMUNICATION & TRAINING

Share remote working security best practices with your employees. Don't assume that they know what's safe and unsafe.

SECURE ACCESS

Ensure employees have secure internet access when working from home and aren't relying on public wifi. When possible, provide corporate VPN access.

DATA STORAGE

Provide your employees with secure data storage options (on-site or cloud-based). Home computers, mobile devices and USB memory sticks are not safe options for storing company data.

MONITORING

When possible, monitor your employees' computer systems remotely to watch for security threats.

CONTINGENCY PLANNING

Be proactive and develop a plan of action for dealing with security issues if they arise. This will help your team stay calm and minimize damage if a crisis occurs.

SERVICE PROVIDERS

Work closely with your IT service providers to assess, mitigate and respond to security issues. They are there to help, so ensure your team knows who to call for support.

Five IT Security Tips for Employees Working from Home

Maintaining IT security requires a team effort.

If your organization has employees working from home, it's important that they know what they can and should be doing to protect themselves and the company.

Here are 5 simple tips you can share with your employees to ensure the whole team is making IT security a priority.

1. **STAY SAFE.** Firewalls, **antivirus software** and virus checkers offer strong protection for your devices and our network, but only if you use them. Be sure to download required IT security software and always run software updates as soon as they're available.

2. **LOCK UP.** IT security threats aren't only online – they're also around us in the real world. Always remember to physically lock your workspace and equipment when you are finished working or simply stepping away from your desk.

3. **KEEP IT PROFESSIONAL.** When it comes to IT security, it's best to keep work and personal separate. For sharing information and files, this means always using your work email and devices, never your personal email or USB memory sticks.

4. **BACK UP.** Your work and files are valuable, so it's important to keep them safe. Remember to regularly back up your work to a secure, company-approved cloud storage system.

5. **ASK FOR HELP.** IT security is all about teamwork, so make sure you know whom to call if something goes wrong with your home office technology. If you have any concerns, it's always better to call – there are no stupid questions!

Four Tips for Protecting Your Business When Employees Work from Home

Having employees working from home adds a new layer of complexity to your organization's IT security environment.

Here are 4 tips for how you can mitigate IT security risk while keeping your team safe and productive, wherever they're working.

1. **USE SECURE VPN TECHNOLOGY.** As the name suggests, a virtual private network (VPN) can give your team access to a private network even when they're working from home. Using a VPN offers many benefits, including encrypted data transfers and hiding of users' locations and IP addresses.

2. **USE MULTI-FACTOR AUTHENTICATION.** This requires users to provide two or more pieces of evidence to access devices or systems, rather than simply a password. Implementing multi-factor authentication for your remote employees can reduce the risk of unauthorized access.

3. **IMPLEMENT ACCESS CONTROL.** For work-from-home employees, limiting their access to only the systems and data they need to do their job helps to minimize risk. Access control allows you to specify who can access what while requiring user authentication.

4. **PROVIDE SECURITY TRAINING.** Security training for your employees can help them understand the IT risks involved in working from home and the best practices that can keep them and the company safe. Sharing a company security policy written in clear, simple terms will help your team understand their responsibilities.

Keeping Your Team Connected Using Online Communication Tools

Online communication tools play a key role in keeping your employees connected and collaborating when they are working remotely, but they come with risks.

In today's work-from-home era, platforms like Zoom, Teams and GoToMeeting have become central to how teams function. Unfortunately, it didn't take hackers long to figure out how to crash online meetings.

Achieving 100% security with online communications is difficult, but there are steps you can take to mitigate risk.

Depending on your organization's needs and preferred platforms, here are some ways to make online communications safer:

- Make all meetings invite only and password protected
- Require all users/participants to be signed in
- Disallow screen sharing for users who don't need to share their screen
- Turn off file sharing
- Turn off annotation
- Create waiting rooms to see who is trying to join the meeting
- Disable video
- Mute all users until they need to say something
- Disable private chat

Making Use of a Secure Cloud Storage System

When you have employees working from home who need remote access to files, cloud storage systems are particularly useful.

However, it's important to keep in mind that they are no more or less secure than on-site solutions – it all comes down to security practices.

Here are some security features that can help you maintain a secure cloud storage system:

- **FILE SYSTEM SNAPSHOTS –** This allows you to make a copy of all the files in part or all of your company's cloud storage at a single point in time, which can then be used as a backup in the event of your cloud storage being damaged or compromised.
- **REMOTE DATA AND ACTIVITY MONITORING –** This allows you to remotely monitor how and when data in your cloud storage is being accessed, and who is accessing it.
- **REMOTE DEVICE ENCRYPTION AND DATA WIPES –** This allows you to control device access remotely using encryption and to wipe data from lost, stolen or compromised devices via the cloud.
- **VIRTUAL DESKTOP INFRASTRUCTURE –** This allows you to control which tools and programs your employees can access on their device as this infrastructure is stored in the cloud. Going beyond simply providing employees access to files stored in the cloud, virtual desktop infrastructure is like a virtual computer.

Security Considerations for a Widespread Remote Team

Having employees working from home is one thing, but what if your team is spread out across different countries?

In general, IT security fundamentals remain the same whether your employees are in the same building or on the other side of the globe. However, having a widespread remote team does raise some additional security considerations:

- **IT SECURITY RESTRICTIONS.** Some countries (e.g. China and some countries in the Middle East) do not allow VPN software and are known for spying on individuals' online activities. If you have employees working in such countries, you may need to implement additional security policies to keep your team, your company and your data safe.

- **SOVEREIGNTY ISSUES.** Where your data is stored can have significant security implications. For example, the US Patriot Act allows the US government to access any data stored on American soil. This means if you have, for example, financial or health data that belongs to employees or clients, you need to ensure that data lives on Canadian soil.

- **COMPLIANCE ISSUES.** Many cloud-based providers do not have data centers in Canada. If you want to be PCI and PIPEDA compliant, this means you may not be able to use certain cloud-based providers.

How to Set Up a Virtual Office in a Hurry

Successful businesses must be nimble, and sometimes you might need to help an employee get a home-based office up and running in a hurry to avoid losing productivity.

Here are 4 tips on how to get this done quickly yet safely:

1. **PROVIDE SUPPORT.** Your employees shouldn't be left to navigate this process on their own. Your IT team or an external IT provider should lead employees through this process to ensure it's done right and in line with your corporate policies.

2. **ASSESS AND MITIGATE RISK.** This needs to happen before employees are given remote access to company resources. Yes, this takes time, but cutting corners here in order to get your team online in a hurry can increase your corporate risk exponentially.

3. **IMPLEMENT SECURE SOLUTIONS.** Creating a secure home-based office requires tools and systems that are up to the job. Ensure your remote employees are utilizing secure connections, secure print devices and virus-protected hardware.

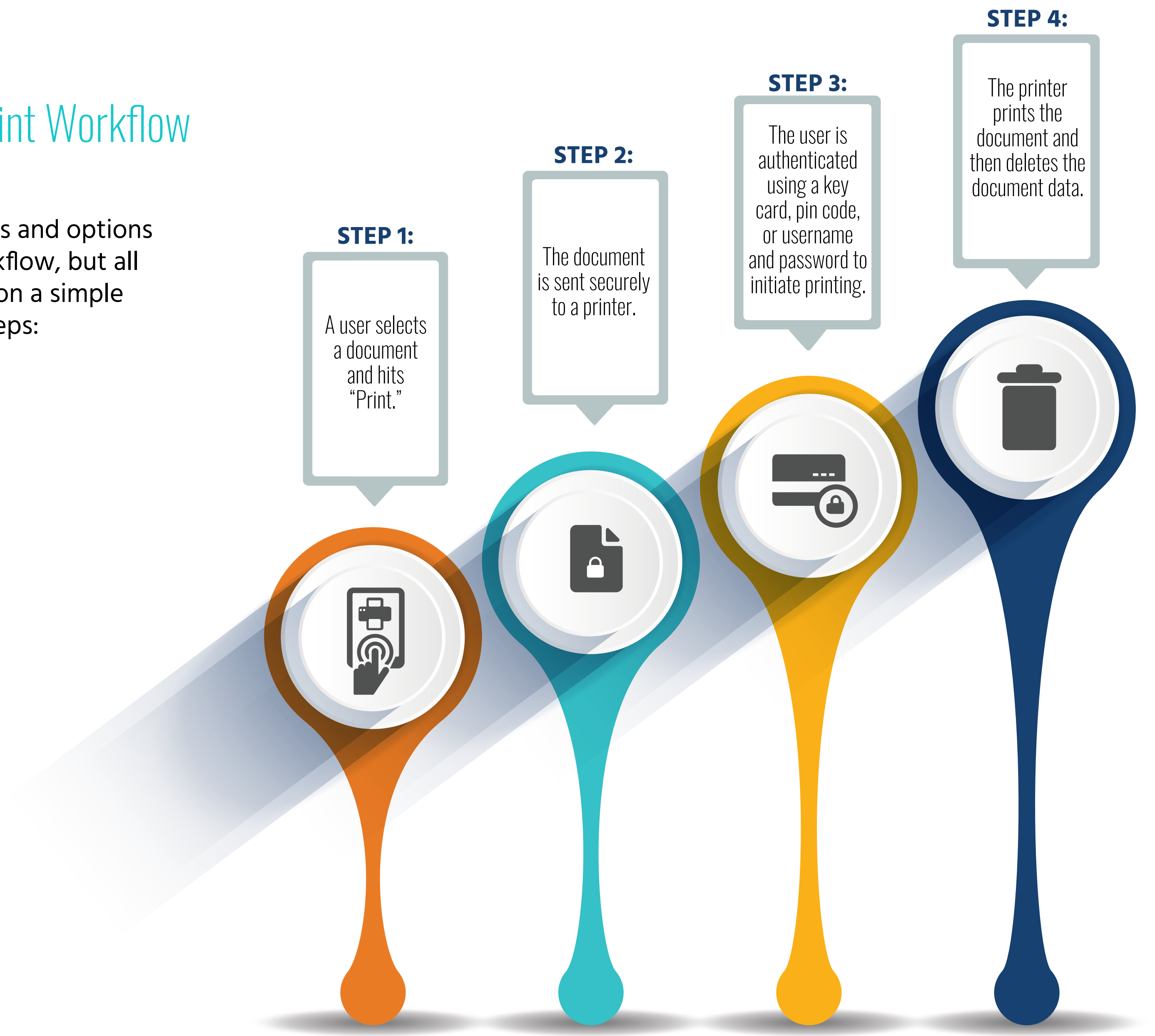
4. **TAKE SECURITY THREATS SERIOUSLY.** Ransomware and other types of security breaches can lead to painful and expensive problems. Even if it seems like the odds of being targeted are low (they're not!), adopting a cavalier attitude toward IT security is a bit like playing Russian roulette.

CHAPTER 3

Secure Workflow

Visualizing a Secure Print Workflow

There are many tools, strategies and options for creating a secure print workflow, but all workflows tend to be centred on a simple process with 4 fundamental steps:



STEP 1: A user selects a document and hits "Print."

STEP 2: The document is sent securely to a printer.

STEP 3: The user is authenticated using a key card, pin code, or username and password to initiate printing.

STEP 4: The printer prints the document and then deletes the document data.

Twelve -Step IT Security Health Check

Maintaining IT security in a corporate environment is an ongoing battle, but you have to start somewhere.

Here are 12 security essentials to help you conduct an initial health check and identify areas for improvement:

1. **SECURITY ASSESSMENT –** Have you recently completed an IT security health assessment?
2. **ENCRYPTION –** Are you applying encryption to your files, emails and mobile devices?
3. **VENDOR SECURITY –** Have you reviewed your vendors' security policies and any potential vulnerabilities from outside sources?
4. **BRING YOUR OWN DEVICE (BYOD)** – Does your company have a process for setting up employees on their own devices, and do they understand what your BYOD policies entail regarding company access to their personal devices?
5. **BACKUPS –** Is your data backed up regularly to secure cloud storage?
6. **SOFTWARE AND COMPUTER UPDATES –** Are your employees and IT team consistent with implementing software updates?
7. **COLLABORATION –** When is the last time you met with your IT team or IT solutions provider to discuss security concerns?
8. **PASSWORDS AND MULTI-FACTOR AUTHENTICATION** – Have you installed multi-factor authentication to protect your network and programs?
9. **SECURITY-ORIENTED CULTURE –** Have you rolled out employee training to teach employees about data security, email attacks, and your company's policies and procedures?
10. **WEB GATEWAY SECURITY –** Are you using a secure web gateway to add an additional layer of protection against web and email threats?
11. **MOBILE DEVICE SECURITY –** Do your employees know how to identify threats and keep your company's data safe on their mobile devices?
12. **FIREWALL –** Is your internal network protected by a strong firewall to control and monitor network traffic?

Developing an IT Security Policy for Your Business

Given the pervasive role of technology in modern businesses, having an IT security policy is just good business sense.

While the specifics should be tailored to the needs of your organization, here are some common components to include in your IT security policy:

- **PREVENTION –** What steps are you taking to proactively identify and mitigate risks?
- **MAINTENANCE –** What needs to be done on an ongoing basis to maintain the effectiveness of your prevention activities?
- **RESPONSE –** What is your plan to respond quickly and effectively if you encounter a security incident?
- **INITIAL TRAINING –** What initial training do you provide to your team and new team members to introduce your company's IT security policies and best practices?
- **ONGOING TRAINING –** What ongoing training do you provide to keep an IT security mindset refreshed and top of mind among your team?
- **MONITORING AND ADHERENCE –** What are your procedures for monitoring your organization's IT security and ensuring adherence to existing policies?

Updating Software with Patch Cycles

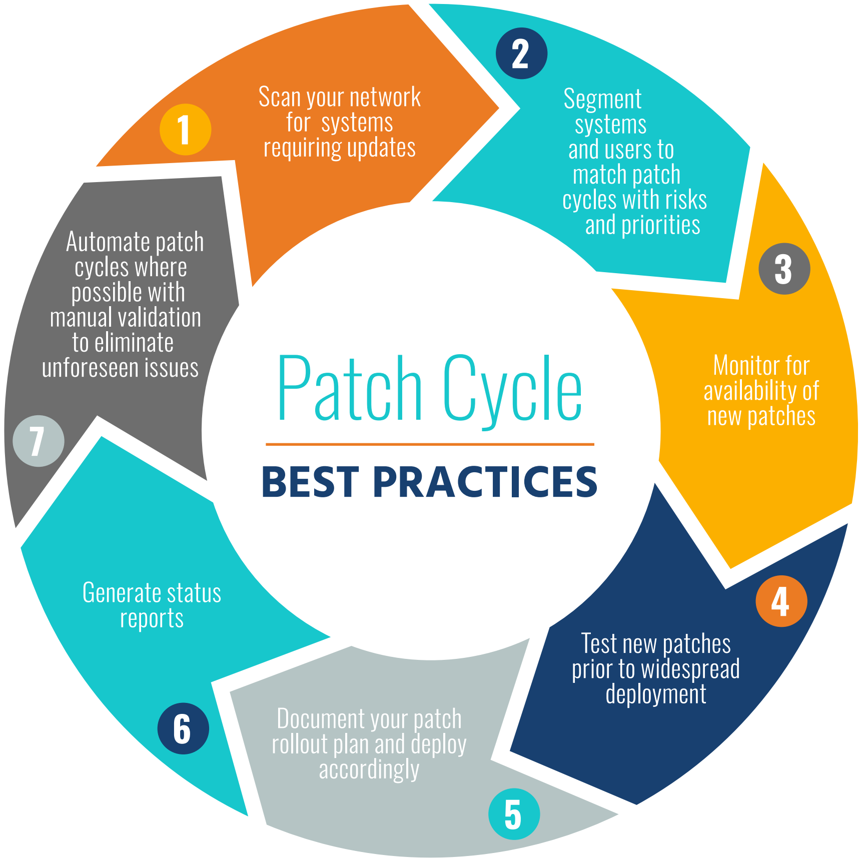
57% of data breaches are attributed to poor patch management (source: Ponemon)

Patch management is the process of distributing and applying updates to software, typically to correct errors in the software.

For businesses, implementing security updates and patches on operating systems, applications and embedded systems (like network equipment) is an essential step in managing IT security.

Since patches are developed on an ongoing basis as errors and vulnerabilities are identified, it's a good idea to establish an ongoing patch cycle for your organization.

Consider these patch cycle best practices.


Patch Cycle
BEST PRACTICES
1
Scan your network for systems requiring updates
2
Segment systems and users to match patch cycles with risks and priorities
3
Monitor for availability of new patches
4
Test new patches prior to widespread deployment
5
Document your patch rollout plan and deploy accordingly
6
Generate status reports
7
Automate patch cycles where possible with manual validation to eliminate unforeseen issues

Implementing Bring Your Own Device (BYOD)

BYOD policies allow employees to use their personal phones, laptops or other devices for work purposes.

For employees, the appeal of BYOD is often the ability to use a familiar device. Companies, on the other hand, like BYOD because it can reduce the need to invest in IT hardware and software.

With BYOD, the employee provides the device, but it's the company that sets the requirements for how to keep the device secure. The following are some of the components commonly found in BYOD policies:

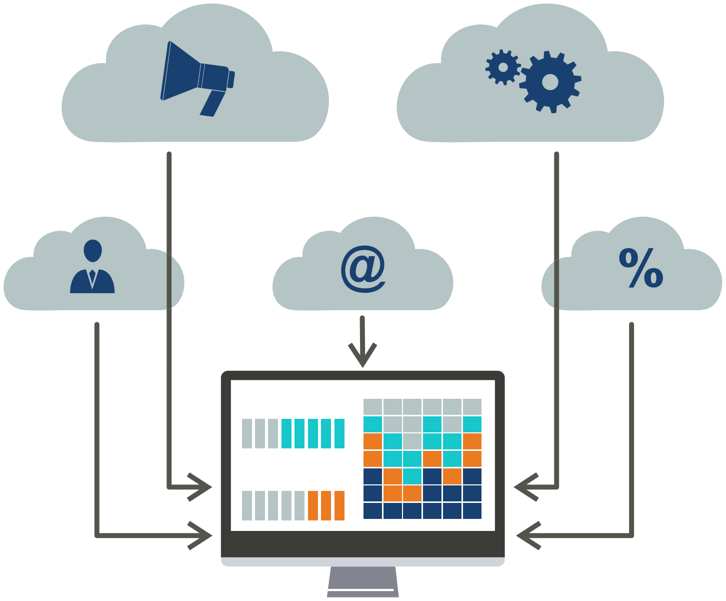
- Compulsory strong passwords
- Prohibited applications
- Restrictions on data access
- Mandatory antivirus software
- Mandatory encryption
- Backup strategy
- Employee education
- Reporting of lost or stolen devices

BYOD Caveat

Before implementing a BYOD policy in your organization, consider this important caveat: at the end of the day, your employee still owns their device and has legal control over it.

This means the only way to ensure 100% compliance with your company's security policies is to avoid BYOD and instead provide 100% of the hardware and software required.

What's Your Business Contingency Plan?



We all hope it never happens to us, but the reality is that any business could suffer a security breach at any time.

As it's impossible to fully mitigate all risk, the next best option is to be well prepared. Enter business contingency planning.

By planning proactively, you can react more quickly and respond more effectively to a crisis, which should help you minimize damage.

Here are some of the components to include in your business contingency plan:

- Documented plans for data backup, replication and disaster recovery
- Identification of key people who need to be informed and who will take on specific responsibilities
- Identification of vital processes, systems and technology to keep the organization running, as well as alternate systems
- Crisis communication plan for keeping stakeholders informed during a crisis
- Regular testing of emergency systems:
  - Are the backups tested regularly?
  - Does your offsite disaster recovery plan work?
  - Do you test offsite replication?
  - Can you spin up your disaster site environment, and is this tested at least once annually?

Phishing Emails and How to Spot Them

Phishing emails are designed to look legitimate, which is precisely why they're so dangerous.

Since phishing emails are made to look like they're coming from a trusted person or institution, spotting them can be a challenge. However, a bit of vigilance and common sense go a long way.

Here are 7 tips to avoid falling victim to a phishing email:

1. Never open attachments you weren't expecting
2. If it looks like it came from someone you know, confirm with a call or in a separate email (not a reply to the original email)
3. If you get an email from a financial institution, treat it with suspicion unless you were expecting it
4. Be careful opening PDF attachments – they may in fact be scripts that execute a virus
5. Be suspicious of emails with links – they are as dangerous as attachments and may lead you to a compromised website
6. Watch for emails that try to scare you into action by threatening a loss of service (e.g. being locked out of an account)
7. Hover over any links in emails or attachments to see where they actually lead – this is likely different from the destination suggested in the email

CHAPTER 4

Creating a Secure Culture

Creating a Secure Culture

Effective IT security is not a one-off event – rather, it's about creating a culture in which everyone understands, thinks about and respects the important of security.

There's no one-size-fits-all approach to developing such a culture, but employee training is a good place to start.

Whether delivered by an internal team or external service provider, security training should be both relevant and engaging.

Training best practices:

- **MAKE IT A PRIORITY –** Employees won't take it seriously if they sense it's just a box-ticking exercise
- **KEEP IT FRESH** – Shorter but more frequent training sessions keep security top of mind better than one long, annual session
- **CUSTOMIZE IT –** Training must be tailored to the realities of your workplace and the types of situations your team may actually encounter

Develop an IT Security Strategy for Your Small Business

IT security is just as important for small businesses as it is for large enterprises. The only difference is the need to adapt policies and practices to your organization's requirements and pain points.

To develop an IT security strategy for your small business, it can help to start by framing your thinking with these three areas:

1. **GOVERNANCE –** Clearly determine and assign roles and responsibilities related to ownership, implementation and operation of security tools.

2. **DATA CLASSIFICATION AND INVENTORY –** Identify what data is important and develop a clear understanding of where the data resides. This is an ongoing process as the data grows and ages out, turning into archival data.

3. **POLICIES –** Define and develop IT security policies that reflect risk and align with business priorities.

Once you have an understanding of these three areas, it becomes easier to understand how to incorporate the following elements of IT security within your organization:

- Configurations and patching
- Secure authentication
- Backups and business continuity
- Access protection
- Monitoring
- Encryption
- Training

Ransomware Prevention, Detection and Remediation

A ransomware attack involves criminals gaining access to your systems, installing malware that locks you out and then demanding a ransom to let you back in.

Most (but not all) ransomware events occur when users are socially engineered into opening attachments or visiting compromised websites.

Regardless of how the perpetrators gain access, the impact of a ransomware attack can be devastating – especially for businesses that are unable to recover or recreate the data and systems that are compromised.

Here are 3 important tips for preventing and dealing with ransomware attacks:

1. **EXTENSIVE AND ONGOING TRAINING IS THE BEST DEFENSE AGAINST RANSOMWARE.** Most ransomware attacks could be prevented by users spotting phishing attempts and maintaining strong passwords.
2. **AN AIRTIGHT BACKUP STRATEGY IS THE ONLY EFFECTIVE WAY TO RECOVER FROM A RANSOMWARE ATTACK.** Forget about paying the perpetrators – as crooks with no scruples, they will likely just take the money and run.
3. **BE SURE TO CONDUCT FORENSICS AFTER AN ATTACK TO FIGURE OUT HOW THEY GOT IN.** If you skip this step, you may end up back where you started soon after you clean up the mess.

CHAPTER 5

Secure Print Network

The ABCs of Print Network Security

Maintaining a secure print network is a key pillar of overall IT security – especially if your organization is in an industry with heightened privacy concerns, such as legal, accounting, insurance or healthcare.

To understand and bolster the security of your print network, start with these ABCs:

A. **ASSESS YOUR INFRASTRUCTURE.** What hardware and software components make up your print network? How do they connect with each other? How up to date or out of date are they?

B. **BOOST WORKFLOW SECURITY MEASURES.** What existing security measures are part of your print workflow? How effective are they? How can you strengthen existing measures or add new ones?

C. **CONSIDER OUTPUT RISKS.** What are the vulnerabilities in your print network? What could go wrong, and what would the implications be if things did go wrong? How are you monitoring output to see who is printing what?

Securing Your Print Network Infrastructure

A secure print network requires a solid foundation. This means securing the hardware and software in your print network before the first job is even sent to print.

Fortunately, today's sophisticated devices and software have powerful tools and settings that can help you maximize the safety of your print network.

For example:

- **FIRMWARE ATTACK PREVENTION AND SELF-RECOVERY –** These tools can identify a malicious intrusion in your print network and automatically restore a machine's firmware to its original state.
- **APPLICATION WHITELISTING –** This tool detects attempts to access a machine's file system and denies access if the source data does not match what is on the whitelist.
- **ACTIVE DIRECTORY GROUP POLICIES –** This tool centrally manages specific security settings, driver settings, restrictions and power management; once applied, these settings cannot be changed at the machine.

Securing Your Print Network Workflow

To realize the full benefits of secure print network infrastructure, it must be paired with a secure workflow.

There are a variety of strategies for securing your workflow with different levels of complexity and safety mechanisms. What makes sense for you will depend on the size of your print network and the security needs of your organization.

Here are a few examples:

- **SECURE USER AUTHENTICATION –** Before printing, employees are required to complete a user authentication process, which may involve using a password, a fob or two-factor authentication. This is a fundamental requirement for a secure print network workflow.

- **SECURE PRINT RELEASE –** This approach holds print jobs in a secure queue and starts printing only once the user completes an authentication process at the printer. By requiring users to be physically present, this reduces the risk of sensitive documents sitting unattended at the printer.

- **FIND-ME PRINTING –** This is a roaming print solution that allows users to print to a single queue and have their jobs “pulled” to any printer where they authenticate. Paired with secure print release, this approach provides flexibility while maintaining security.

Securing Your Print Network Output

To secure your print network output, you need to monitor and understand how the network is being used. There are different ways to do this, depending on the level of detail and oversight you require.

PRINT AUDITING. Print networks typically offer at least some capabilities for auditing of printer output. At a basic level, this may include only data such as the time, date and number of pages for each job. More sophisticated auditing can provide more detailed usage analytics.

PRINT ARCHIVING. This is a powerful solution that uses image-capture technologies to create a comprehensive record of all printed documents. This information is organized in a job log, which can sort print jobs by attributes such as printer, account and user.

Print archiving offers numerous benefits and can be used in a variety of ways, including:

- Creating a detailed record of all printed materials
- Allowing easy searching and viewing of past print jobs
- Reprinting of specific documents or pages from the print archive
- Activating print archiving for only specified printers and users
- Meeting regulatory requirements for handling of sensitive data

COM · PRO
Managed Business Solutions

CONTACT US

Head Office:
18515 53rd Avenue
Suite 110
Surrey, BC, V3S 7A4

TF: 1-866-266-7761
T: 604-574-8623
F: 604-574-8634

Vancouver Office:
1108 W 8th Avenue
Vancouver, BC, V6H 3Z5

T: 604-664-8901
F: 604-900-3377