TECHNOLOGY UPDATE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

INSIDE THIS ISSUE

This monthly publication is provided courtesy of Amanda & Bryan Lachapelle, owners of B4 Networks.

HEADQUARTERS

160 Hwy 20 W. Unit 10, Box #249
Fonthill, Ontario, L0S 1E0
(905) 228-4809

BARRIE LOCATION

30 Quarry Ridge Road
Barrie, Ontario, L4M 7G1
(705) 885-0993

SHADOW IT:

How Employees Using Unauthorized Apps Could Be Putting Your Business At Risk

Your employees might be the biggest cybersecurity risk in your business – and not just because they're prone to click phishing emails or reuse passwords. It's because they're using apps your IT team doesn't even know about.

This is called Shadow IT, and it's one of the fastest-growing security risks for businesses today. Employees download and use unauthorized apps, software and cloud services – often with good intentions – but in reality they're creating massive security vulnerabilities without even realizing it.

What Is Shadow IT?

Shadow IT refers to any technology used within a business that hasn't been approved, vetted or secured by the IT department. It can include things like:

- Employees using **personal Google Drives or Dropbox accounts to store and share work documents.**
- Teams signing up for **unapproved project management tools** like Trello, Asana or Slack without IT oversight.

continued on page 2...

...continued from cover

- Workers installing **messaging apps like WhatsApp or Telegram** on company devices to communicate outside of official channels.

- Marketing teams using **AI content generators** or automation tools without verifying their security.

Why Is Shadow IT So Dangerous?

Because IT teams have no visibility or control over these tools, they can't secure them – which means businesses are exposed to all kinds of threats.

- **Unsecured Data-Sharing** – Employees using personal cloud storage, email accounts or messaging apps can accidentally leak sensitive company information, making it easier for cybercriminals to intercept.

- **No Security Updates** – IT departments regularly update approved software to patch vulnerabilities, but unauthorized apps often go unchecked, leaving systems open to hackers.

- **Compliance Violations** – If your business falls under regulations like PIPEDA, GDPR or PCI-DSS, using unapproved apps can lead to noncompliance, fines and legal trouble.

- **Increased Phishing And Malware Risks** – Employees might unknowingly download malicious apps that appear legitimate but contain malware or ransomware.

- **Account Hijacking** – Using unauthorized tools without multifactor authentication (MFA) can expose employee credentials, allowing hackers to gain access to company systems.

Why Do Employees Use Shadow IT?

Most of the time, it's not malicious. Take, for example, the "Vapor" app scandal, an extensive ad fraud scheme recently uncovered by security researchers IAS Threat Lab.

In March, over 300 malicious applications were discovered on the Google Play Store, collectively downloaded more than 60 million times. These apps disguised themselves as utilities and health and lifestyle tools but were designed to display intrusive ads and, in some cases, phish for user credentials and credit card information. Once installed, they hid their icons and bombarded users with full-screen ads, rendering devices nearly inoperative. This incident highlights how easily unauthorized apps can infiltrate devices and compromise security.

But employees can also use unauthorized apps because:

- They find company-approved tools frustrating or outdated.

- They want to work faster and more efficiently.

- They don't realize the security risks involved.

- They think IT approval takes too long – so they take shortcuts.

Unfortunately, these shortcuts can cost your business BIG when a data breach happens.

How To Stop Shadow IT Before It Hurts Your Business

You can't stop what you can't see, so tackling Shadow IT requires a proactive approach. Here's how to get started:

1. Create An Approved Software List

Work with your IT team to establish a list of trusted, secure applications employees can use.

Make sure this list is regularly updated with new, approved tools.

2. Restrict Unauthorized App Downloads

Set up device policies that prevent employees from installing unapproved software on company devices. If they need a tool, they should request IT approval first.

3. Educate Employees About The Risks

Employees need to understand that Shadow IT isn't just a productivity shortcut – it's a security risk. Regularly train your team on why unauthorized apps can put the business at risk.

4. Monitor Network Traffic For Unapproved Apps

IT teams should use network-monitoring tools to detect unauthorized software use and flag potential security threats before they become a problem.

5. Implement Strong Endpoint Security

Use endpoint detection and response (EDR) solutions to track software usage, prevent unauthorized access and detect any suspicious activity in real time.

Don't Let Shadow IT Become A Security Nightmare

The best way to fight Shadow IT is to get ahead of it before it leads to a data breach or compliance disaster.

Want to know what unauthorized apps your employees are using right now? Start with a Cybersecurity Assessment to identify vulnerabilities, flag security risks and help you lock down your business before it's too late.

How Does Your IT Company Compare?

Our May 2025 Help Desk Key Performance Indicators

100%

Client Satisfaction

31 Mins

Average Response Time

IS YOUR PRINTER THE BIGGEST SECURITY THREAT IN YOUR OFFICE?

If I asked you to name the biggest cybersecurity threats in your office, you'd probably say phishing emails, malware or weak passwords. But what if I told you that your office printer – yes, the one quietly humming in the corner – could be one of the biggest vulnerabilities in your entire network?

It sounds ridiculous, but hackers love printers. And most businesses don't realize just how much of a security risk they pose – until it's too late. In 2020, Cybernews ran what they called the "Printer Hack Experiment." Out of a sample of 50,000 devices, they successfully compromised 56% of the printers, directing them to print out a sheet on printer security. That's nearly 28,000 compromised devices – all because businesses overlooked this "harmless" piece of office equipment.

Wait, WHY Target Printers?

Because printers are a goldmine of sensitive data. They process everything from payroll documents and contracts to confidential client information. And yet, most businesses leave them wide-open to attack.

Here's what can happen when a hacker gains access to your printer:

- **Printers store sensitive data** – Every time you print, scan or copy a document, your printer keeps a digital copy. Many printers have built-in hard drives that store years' worth of documents, including payroll files, contracts and employee records. If a hacker gains access, they can steal or even reprint those files without your knowledge.

- **Default passwords are a hacker's dream** – Most printers come with default admin logins like "admin/admin" or "123456." Many businesses never change them, making it easy for cybercriminals to take control.

- **They're an open door to your network** – Printers are connected to your WiFi and company network. If compromised, they can be used as an entry point to install malware or ransomware, or steal data from other devices.

- **Print jobs can be intercepted** – If your print jobs aren't encrypted, hackers can intercept documents before they even reach the printer. That means confidential contracts, legal documents and even medical records could be exposed.

- **They can spy on your business** – Many modern printers have built-in storage and even scan-to-email features. If a hacker compromises your device, they can remotely access scanned documents, emails and stored files.

- **Outdated firmware leaves the door wide-open** – Like any device, printers need security updates. But most businesses never update their printers' firmware, leaving them vulnerable to known exploitations.

- **Data mining from discarded printers** – Printers that were improperly disposed of can be a goldmine for cybercriminals. Residual data stored on discarded printers can be mined for sensitive information! This can result in potential security breaches. Printers need to have their storage wiped clean to avoid being vulnerable to data breaches and legal liabilities.

How To Protect Your Printers From Hackers

Now that you know printers can be hacked, here's what you need to do immediately:

1. Change The Default Password – If your printer still has the default login credentials, change them immediately. Use a strong, unique password like you would for your email or bank account.

2. Update Your Printer's Firmware – Manufacturers release security patches for a reason. Log into your printer settings and check for updates or have your IT team do this for you.

3. Encrypt Print Jobs – Enable Secure Print and end-to-end encryption to prevent hackers from intercepting print jobs.

4. Restrict Who Can Print – Use access controls so only authorized employees can send print jobs. If your printer supports PIN codes, require them for sensitive print jobs. You can also add a guest option.

5. Regularly Clear Stored Data – Some printers let you manually delete stored print jobs. If yours has a hard drive, make sure it's encrypted, and if you replace a printer, wipe or destroy the hard drive before disposal.

6. Put Your Printer Behind A Firewall – Just like computers, printers should be protected by a firewall to prevent unauthorized access.

7. Monitor Printer Activity – If your IT team isn't already tracking printer logs, now is the time to start. Unusual print activity, remote access attempts or unauthorized users printing sensitive documents should be red flags.

Printers Aren't Just Office Equipment – They're Security Risks

Most businesses don't take printer security seriously because, well, it's a printer. But cybercriminals know that businesses overlook these devices, making them an easy target.

If you're protecting your computers but ignoring your printers, you're leaving a huge hole in your cybersecurity defenses.

VACATION SEASON, IT EMERGENCY

It's a quiet June morning. Half your team is on vacation. The other half is working from home or bouncing between coffee shops and hotel WiFi. And then it happens.

- Your system goes down.
- The printer stops working.
- No one can access shared files.
- A phishing e-mail just landed in someone's inbox.

You call your IT person – and they're out of office too. Now what?

Your business is frozen, and there's no one available to fix it. Sound dramatic? Maybe. But unrealistic? **Not even a little.**

Summer's Great For Fun, And Terrible For Reactive IT Support

Most business owners don't realize how much goes into keeping their business up and running, until something breaks – and the only person who knows how to fix it is sipping daiquiris on a beach somewhere without a cell phone signal in sight.

That's the main problem with **reactive IT support**. It works fine…until it doesn't. And then you're left scrambling to repair the damage.

When your tech strategy is based on "Just call Bob if something goes wrong," you're taking a huge risk. Especially in the summer, because tech problems don't care about PTO.

- Servers still crash.
- Hardware still overheats.
- Hackers still send e-mails.

And when no one's there to respond quickly, the damage stacks up – **fast**.

Reactive IT = Constant Firefighting

When you rely on a "fix-it-when-it-breaks" approach:

- Downtime drags on while you wait for someone to become available.
- Cyberthreats slip through the cracks because no one is actively monitoring systems.
- Small issues snowball into major headaches (and big expenses).
- You have no fallback when your go-to IT person is unavailable.

And in June, when vacations peak and remote work is more common, it's the perfect storm. Instead, you need to work with a company that takes a proactive approach to IT support.

Proactive IT = Business Continuity, Even When You're On The Beach

A proactive IT partner doesn't just wait for things to go wrong. They anticipate issues, prevent disruptions and make sure there's a plan (and people) in place when your usual support is AWOL.

With a proactive team, you get:

- 24/7 system monitoring and maintenance
- Security updates before you're exposed
- Regular backups and disaster recovery plans
- A team of experts – not just one person – with backup coverage
- Predictable costs and fewer surprises

The Cost Of Waiting Until It's Broken

Downtime costs small businesses anywhere from hundreds to thousands of dollars PER MINUTE. Cyberattacks can be even worse, both financially and reputationally.

Waiting until things go wrong isn't just inconvenient; it's risky and potentially expensive.

Ready To Vacation Without Worry?

This summer, don't leave your business exposed while your team (or your IT support) is away. Let's take a look at your setup and show you how a proactive approach can save you time, money and stress.

DON'T FALL FOR THIS TRAVEL SCAM

Cybercriminals are exploiting travel season by sending fake booking confirmations that look like legitimate emails from airlines, hotels and travel agencies. These scams steal personal and financial information and spread malware.

How The Scam Works

1. A Fake Booking Confirmation Lands In Your Inbox

- Appears to be from travel companies like Expedia, Delta or Marriott.
- Uses official logos, formatting and fake customer support numbers.
- Subject lines create urgency, such as: *"Your Flight Itinerary Has Changed – Click Here For Updates"*

2. Clicking the Link Redirects You To A Fake Website

- Email prompts you to log in to confirm details, update payment info or download an itinerary.
- The link leads to a fraudulent website that steals your credentials.

3. Hackers Steal Your Information/Money

- Entering login credentials grants hackers access to your airline, hotel or financial accounts.
- Providing payment details leads to stolen credit card information or fraudulent charges.
- Clicking malware-infected links can compromise your entire device.

Why This Scam Works

It Looks Legit – Uses real logos, formatting, and familiar-looking links.

It Creates Urgency – "Reservation issues" or "flight changes" cause panic, making victims act fast.

People Are Distracted – Busy travellers often don't double-check emails.

It's A Business Risk Too – If employees handling company travel fall for it, businesses face financial loss and security breaches.

How To Protect Yourself And Your Business

- **Always Verify Before Clicking** – Visit the airline or hotel's website directly.
- **Check The Sender's Address** – Scammers use slightly altered domains (e.g., "@delta com.com" instead of "@delta.com").
- **Educate Your Team** – Train employees to recognize phishing scams.
- **Use Multifactor Authentication (MFA)** – Adds an extra security layer.
- **Secure Business email Accounts** – Block malicious links and attachments.