TECHNOLOGY TIMES

Insider Tips to Help Your Business Run Faster, Easier and More Profitably

Thomas Hill, President & Founder

"A key to getting more done is being able to pay attention to details without getting bogged down in them at the same time!"

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 e-mails 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.

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, e-mail 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 HIPAA, GDPR or PCI-DSS, using unapproved apps can lead to noncompliance, fines and legal trouble.

continued on pg.2

continued from cover

- **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 Labs.

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.

*"CD Technology is tops in their field! We love knowing that someone is behind us and our data. Not only that, but the quality of service has been excellent. Everyone is treated well when needing assistance. **Issues are handled in a timely manner.** I unreservedly recommend CD Technology."*

Steve Haney
Heartland Services

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 Network Security Assessment to identify vulnerabilities, flag security risks and help you lock down your business before it's too late.

Is Your Printer The Biggest Security Threat In Your Office?

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. 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**
- ⇒ **Default passwords are a hacker's dream**
- ⇒ **They're an open door to your network Print jobs can be intercepted**
- ⇒ **They can spy on your business**
- ⇒ **Outdated firmware leaves the door wide -open**
- ⇒ **Data mining from discarded printers**

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 e-mail 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.

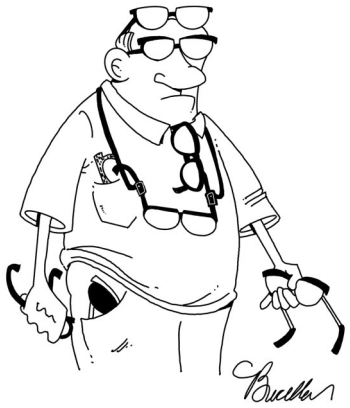
6. Put Your Printer Behind A Firewall – Just like computers, printers should be protected by a firewall to prevent unauthorized access.

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.



Somewhere between middle-age and senior citizen

Here is your chance to win Lunch On Us!
This Month's

TRIVIA

Which US President was also the father of 15 children?

Email your answer to RHill@CDTechnology.com

Happy Father's Day

to all the special men in our lives who are out there living their best dad and granddad life!

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com

A High-Tech Heist for the History Books

The worst mistake you ever made at work can't compare to the one that Ben Zhou, CEO of the cryptocurrency exchange Bybit, made on the evening of Feb. 21.

Zhou merely approved a routine transaction, transferring large amount of the digital currency Ether into another account.

Just 30 minutes later Bybit's chief financial officer dropped a bomb: Their systems had been hacked, and cybercriminals had looted all of Bybit's 500,000 tokens, worth about $1.5 billion.

It was the largest cryptocurrency heist to date. Within just a few hours, blockchain analyst ZachXBT had identified the attackers: the notorious North Korean state-backed Lazarus Group.

The hackers' approach was surprisingly mundane, according to CCN. Bybit relied on free software to safeguard customer deposits. Experts say that the widely-used software, developed by the technology provider Safe, is fine for individuals and hobby traders, but wasn't appropriate for protecting billions in customer deposits.

Cybersecurity experts sounded the alarm. The attack was "completely preventable." After the attack, Bybit customers withdrew nearly $10 billion, about half its total deposits. Zhou rushed to reassure them

that their funds remained available and secure. Three days later, Bybit had recovered $1.23 billion worth of stolen tokens and frozen more than $40 million in still-missing funds. But despite the rapid recovery, the incident still rocked the crypto markets.

There are national security concerns too. Twenty percent of those funds, or about $300 million, vanished. It's impossible to say how the North Korean government will use the stolen funds.

WELCOME

We want to officially welcome K & J Concrete Polishing to our CD Technology community. K & J Concrete Polishing, Inc. specializes in the restoration and refinishing of many different types of concrete floors. They provide the highest quality concrete grinding and polishing in the industry by staying on top of the newest developments in technology and continuous training.

WE ARE MAKING A BIG MOVE

CD TECHNOLOGY

COMING SOON
A NEW, LARGER, CENTRALLY-LOCATED TECHNOLOGY COMMAND CENTER

Announcing...

Exclusively for CDT clients! Do You Have a special event you would like to share with the community? Are you planning an open house, blood drive, block party, anniversary celebration, meet & greet… or any lead generating event open to the public? Let us help you get folks there. We would love to help you promote your special occasion by putting it in our next newsletter and share on all our socials! Just give us the details - make sure to include contact info and we will share your news.

Culture and Trust: A $1M Growth Formula

When it comes to entrepreneurship, sometimes your biggest obstacle is you—and getting out of your own way and empowering employees is the recipe for success. Here are a few tried-and-true entrepreneurial mindset shifts from other business owners that pushed them closer to success.

The Biggest Entrepreneurial Challenge: Delegation

Learning how to step away—and get out of your own way—is one of the biggest lessons many entrepreneurs must learn. When you start a business, you're running everything. You're wearing all the hats. However, in order to grow, you have to face the fact that there's only so much time in a day. You simply don't have time to work in the trenches *and* scale the business.

Hiring good, capable people and *trusting* them enough to take tasks off your plate is critical to your business' success. After all, as the company's leader, it's important to *strategically* spend your time—not just stay busy. Delegate what you can, and focus on setting the vision and strategies that will keep your business moving forward.

Shaping the Culture with a Family Dynamic

There are a few factors that are key to a healthy company culture. An open line of communication is one of the biggest. Listening to what your team needs—even if it's unconventional—and giving it a fair shot can make all the difference. Just be sure to clarify up front that if productivity or the quality of your deliverables slips, it'll be straight back to the way things were before.

If it works, your business has a thriving new dynamic, potentially increasing productivity and workplace satisfaction. But even if it doesn't, your team will feel heard, respected, and like you've got their backs. And that makes all the difference when it comes to creating a strong, trust-based company culture.

If you're not sure where to go next, don't underestimate the value of picking up some books on creating a strong culture. Take advice from entrepreneurs who have been there, done that, and begin incorporating the ideas you like best into your own business. After all, if it worked for them, it might just work for you.

Focus on "Done", Not "Perfect"

From creating processes to marketing, things are better done than perfect. Perfectionism can seriously hold you back. Instead, come up with a plan and implement something. It doesn't have to be exactly right. You can always make tweaks along the way, but if you never take the leap and execute, you'll never get anywhere. So put the planning notebook down, and get implementing!

Entrepreneurship will never be the easy road, but with some essential shifts to your mindset and a great team around you, many challenges don't seem quite so insurmountable.

IMPORTANT NEWS:

Windows 10 Support Ends In 2025 – What Are Your Options?

In 2025, Microsoft will stop providing critical services like security updates, leaving your business vulnerable to threats and potential downtime.

Here Are Your Options:

- **Upgrade To Windows 11**
  Not all devices will be compatible, so make sure to check with an IT expert.
- **Buy A New PC**
  For businesses with older machines, a hardware upgrade might be your best bet.
- **Pay For Extended Security Updates**
  Only available for up to three years (and it's not free).
- **Switch To Linux**
  For those willing to explore new systems.
- **Do Nothing (NOT RECOMMENDED!)**
  This could expose your business to cyber risks and compliance violations.

Don't Gamble With Your Business!
Plan Your Next Steps Today

Call

865-909-7606

CLASS OF 2025

You did it!

May you have much success and happiness as you begin your next chapter whatever that may be.

CD TECHNOLOGY
10721 Chapman Hwy #30
Seymour, TN 37865

June 2025

INSIDE THIS ISSUE

Strawberry Pie, Oh My!

INGREDIENTS:

Filling

1 small box Strawberry Jello
4 Tbs flour
1 cup sugar
1 cup water
1-pint or more (how high do you want your pie?) fresh strawberries, halved or quartered, set aside the prettiest ones for the top of the pie. Keep your berries cold.

Cream Cheese Layer

½ block of softened cream cheese mixed with about a ½ c sugar.
1tsp vanilla
¼ c vanilla yogurt folded in to WELL BLENDED mixture

PREPERATION:

Obtain some really good, fresh strawberries. Go pick some. Your pie will thank you!
Bake a deep dish pie shell, add the cream cheese mixture on the bottom after it has cooled.
Wisk Jell-O, sugar, water and flour. Cook slowly until dissolved and begins to bubble, it should be thick.
Remove from heat and add strawberries.
Spoon over cream cheese mixture.
Make it pretty. You are a food artist!
Refrigerate 3-4 hours or until set.
Top with squirty whipped cream on individual slices.
This is the only way! Do not insult your beautiful pie with whipped topping!

SERVES: 8 slices which is never enough!