TECHNOLOGY EDGE

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

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

continued on page 2...

...continued from cover

- **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.

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

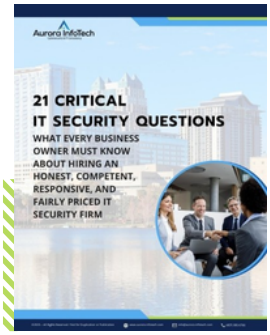
The best way to fight Shadow IT is to get ahead of it before it leads to a data breach or compliance disaster.

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.

FREE REPORT:

What Every Small-Business Owner Must Know About Hiring An Honest, Competent, Responsive and Fairly Priced IT Security Firm

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.



Download your FREE copy today at wwww.aurora-infotech.com/21-questions-free-report/ or call our office at (407) 995-6766.

CARTOON OF THE MONTH

"I understand your concerns, but there's a chain of command. Have you spoken to the sheepdog?"

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.

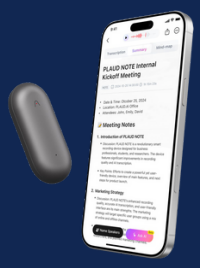
Focus On "Done", Not "Perfect"

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.

SHINY NEW GADGET OF THE MONTH

PLAUD NotePin



Your voice recorder just got way smarter. The PLAUD NotePin combines a wearable digital voice recorder with an AI notetaking assistant, all in one small device. Plus, its sleek, versatile and lightweight design lets you wear it in several different ways: bracelet, necklace or lapel pin.

With the press of a button, it will create advanced, accurate transcriptions in over 112 languages, complete with labels for different speakers. You can also choose your preferred large language model, such as GPT-4o or Claude 3.5 Sonnet, for the NotePin to use.

CLIENT SPOTLIGHT:

Resolved Account Hack When Others Failed!!

I came to Aurora InfoTech after I'd been unsuccessful multiple times trying to gain access to my G-Suite. My email account was highjacked after receiving an email from a client whose account was compromised. Up to that point, Google had been of little help, and since my email accounts were disabled and locked down, I was locked out of everything including a good portion of correspondence for my business. This was going on for nearly three weeks having myself, my technician and my web person attempt unsuccessfully to restore my accounts.

Roy Richardson at Aurora InfoTech was able to provide direction and support I needed to fully recover my account. After everything, I was up within a matter of 24 hours.

-Dawn R. J.Business Training

CYBER LIABILITY ESSENTIALS: WHAT IT IS—AND WHY IT MATTERS MORE THAN EVER

Cybersecurity is no longer just about preventing attacks. It's about documenting your defense, proving your diligence, and preparing for what happens after a breach. That's the foundation of Cyber Liability Essentials—a framework developed to help businesses navigate today's complex legal, regulatory, and insurance environments with confidence.

Here at Aurora InfoTech, we built this solution to bridge the gap between security and liability, especially for small to mid-sized businesses in Central Florida who often face enterprise-level risks without enterprise-level resources.

When the Breach Hits... You're Not Just a Victim Anymore

In the past, being the "victim" of a cyberattack was enough to inspire sympathy. Today, it can make you the defendant in a lawsuit or audit. Increasingly, businesses are being held responsible not just for what happened, but for what they failed to do beforehand.

This means regulatory bodies, insurance carriers, and even clients will be asking questions like:

- What steps did you take to protect the data?
- What training did your employees receive?
- When was the last time your incident response plan was tested?
- Where is the documentation to prove it?

These aren't hypotheticals. These are the real questions clients across industries are now facing—and the ones Cyber Liability Essentials is designed to answer.

The Five Core Protections Behind Cyber Liability Essentials

To make your cybersecurity legally defensible—not just technically sound—Cyber Liability YEssentials focuses on these five pillars:

1. Security Awareness Training That Drives Behavior Change

Most breaches start with human error. That's why traditional "check-the-box" training isn't enough. The Essentials framework delivers ongoing, behavior-based education that helps employees recognize real-world threats and respond correctly in the moment.

2. Enforced, Customized Acceptable Use Policies (AUPs)

Your policies should do more than exist—they should protect you. An AUP tailored to your business provides clear technology usage guidelines and a first line of legal defense when an employee misuses company resources or data.

3. A Realistic and Relevant Incident Response Plan (IRP)

A binder on a shelf won't help in a crisis. Your IRP needs to be personalized to your actual systems, risks, and workflows. It should include specific playbooks for likely threats—so your response is immediate, coordinated, and defensible.

4. A Secure Repository for Documentation and Evidence

Too often, important cybersecurity documentation—like training logs and policies—are stored on the same network they're meant to protect. Essentials ensures that critical files are stored securely, off-site, and accessible even during a full-system outage.

5. Proof of Execution for Every Control

In the eyes of a regulator or insurance adjuster, a policy without proof is the same as no policy at all. Cyber Liability Essentials prioritizes not just implementation, but recordkeeping. This includes detailed logs, audit trails, and ongoing verification that your controls are being followed.

How This Supports Regulatory Compliance and Insurance Readiness

Beyond protecting operations, Cyber Liability Essentials is a powerful foundation for meeting industry and legal standards such as:

- HIPAA
- PCI DSS
- FTC Safeguards Rule
- SEC Cybersecurity Rules
- CMMC (Cybersecurity Maturity Model Certification)

It also supports your standing with cyber insurance providers, many of whom are tightening their requirements and raising their expectations around documentation and due diligence.

Why Documentation Matters as Much as Protection

Cyber Liability Essentials is built on a simple truth: You can't defend what you can't document. It's not enough to have firewalls and antivirus software. In today's legal and compliance environment, businesses need:

- Verifiable training logs
- Updated policies with version control
- Active monitoring and response plans
- Secure storage of documentation
- Clear evidence of ongoing enforcement

This approach shifts cybersecurity from a passive checkbox to an active, auditable program—one that strengthens resilience and positions your business for regulatory and contractual success.