www.hdtech.com JUNE 2025

THE HD TECH WAY

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 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. (see CAM later in this story)

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. Don't have users with local admin privileges.
In the olden days-like 2022-users were allowed to install apps on their own from their computers. In today's malicous cyber world that is too great of a risk. Users need to have their admin rights removed. H&D employs a software call CAM (conditional access management) to only allow a set list of apps to be installed and to allow users to request and get approval to install from the helpdesk- without calling or chatting!

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.

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.

CLIENT SPOTLIGHT:

Sign Printing Company-LA

Recently a new client came onboard and as part of our onboarding we quoted them a new Fortinet Firewall. These standard firewalls for H&D are top tier and have a distinct advantage over less sophisticated firewalls from Sonicwall and Watchguard. Since most attacks today are started from the network, you need a firewall that watches network traffic with a Security Operations Center-like the Fortinet. Besides watching the endpoints it is imperative to be able to see and respond to network based threats.

WHAT'S NEW

This monthly publication is provided courtesy of Tom Hermstad, President & CEO of H&D Technologies.

I recently had the pleasure of attending and delivering a speech at the Annual meeting of the California Independent Petroleum Association (CIPA for short). In the speech, I outlined and broke down the active warzone that is Cyber Security, shedding light on the bad actors and criminal organizations praying upon American businesses. If you missed me, don't fret! We'll be uploading clips in the coming weeks, keep an eye on the website for more details.
Stay safe, and remember, "It's not if...it's when."

To hear more about the War on Cyber or to speak to me, follow the link (www.hdtech.com/meet-tom/). If you're interested in having me speak at an event, email info@hdtech.com.

LEARNING ABOUT SUPPLY CHAIN ATTACKS - WHAT ARE THEY AND WHY DO YOU CARE?

Supply Chain
Raw Material
Supplier
Factory
Distribution
Retail
Customer

Designed by FREEPIK

The Importance of Cyber Preparation in Business Partnerships

Ensuring Security in a Connected World
In today's interconnected business landscape, the importance of cybersecurity cannot be overstated. As businesses become increasingly reliant on digital operations, the threat of cyber attacks looms larger than ever. However, while many companies focus on bolstering their internal defenses, it is equally crucial to engage in open discussions about cybersecurity with vendors, clients, and other business partners. This collaborative approach is essential in safeguarding not only individual entities but the entire network of interconnected businesses.

The Importance to Our Clients

At HDtech.com, we emphasize the significance of comprehensive cyber preparation to our clients. A single vulnerability in the supply chain can jeopardize the security of the entire network. By fostering a culture of open communication and collaboration with business partners, clients can ensure that all parties are aligned in their cybersecurity efforts. This proactive approach not only mitigates risks but also strengthens trust and confidence among stakeholders.

Understanding Supply Chain Attacks
One of the most critical aspects of cyber preparation is understanding the concept of a "supply chain attack." This type of attack occurs when an adversary targets the less secure elements within a supply chain to gain access to the primary target. The consequences of such breaches can be far-reaching, affecting not only the compromised entity but also its business partners and clients. To mitigate this risk, it is imperative for businesses to work closely with their partners to identify and address potential vulnerabilities.

Complimentary Network Assessment

As part of our commitment to enhancing cybersecurity, HDtech.com is offering a free network assessment to our clients and their business partners. This comprehensive evaluation will identify potential weaknesses in the network and provide actionable recommendations to fortify defenses. By availing themselves of this offer, businesses can gain valuable insights into their current security posture and take the necessary steps to enhance their resilience against cyber threats.

The Role of Business Partners in Cyber Preparation

Cybersecurity is not a solitary endeavor. It requires the collective effort of all parties within the business ecosystem. Engaging in regular discussions with vendors, clients, and other business partners about cyber preparation is essential for several reasons:

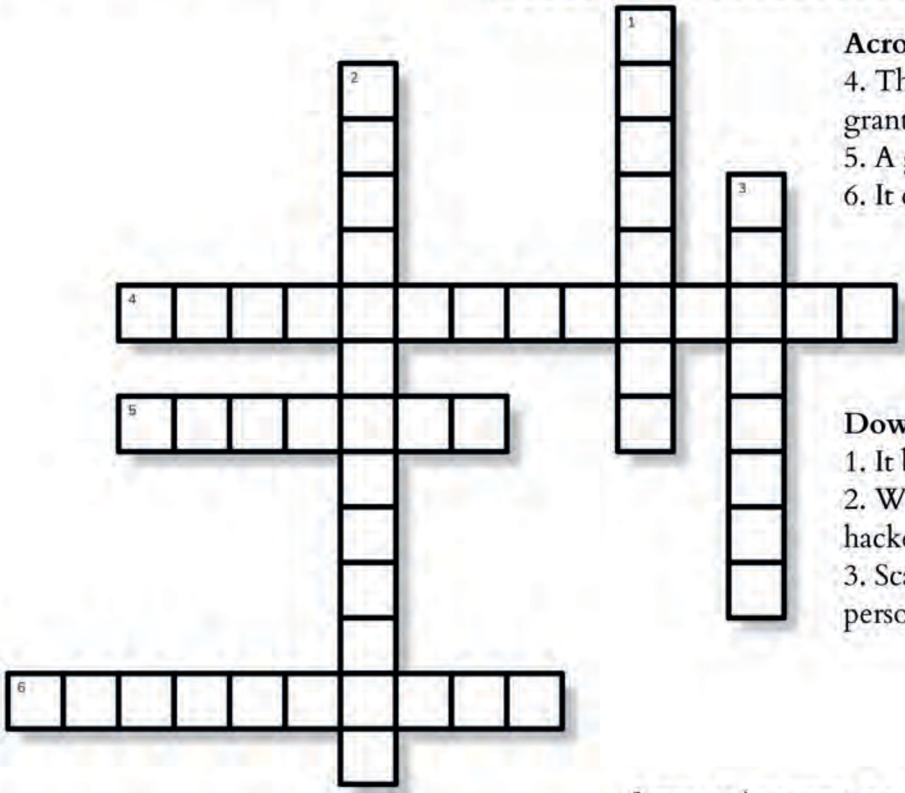
- Shared Responsibility: Cybersecurity is a shared responsibility. By collaborating with partners, businesses can ensure that everyone is aware of their roles and responsibilities in maintaining a secure environment.
- Identifying Weak Links: Regular communication helps identify potential weak links in the supply chain. By addressing these vulnerabilities proactively, businesses can prevent potential breaches.
- Building Trust: Open discussions about cybersecurity build trust and transparency among business partners. This trust is crucial for maintaining long-term relationships and ensuring mutual success.
- Staying Informed: The cyber threat landscape is constantly evolving. By engaging with partners, businesses can stay informed about the latest threats and best practices, ensuring they remain one step ahead of potential attackers.

Conclusion

The importance of talking to vendors, clients, and other business partners about cyber preparation cannot be overstated. As the threat landscape continues to evolve, businesses must adopt a collaborative approach to cybersecurity.

By fostering open communication and offering resources such as free network assessments, HD Tech is committed to helping our clients and their partners build robust defenses against cyber threats. Together, we can create a secure and resilient business ecosystem, ready to face the challenges of the digital age.

TECH TERM TANGLE CROSSWORD TIME



Across

4. The process of verifying one's identity before granting access
5. A general term for malicious software
6. It converts plain text into code to protect data

Down

1. It blocks unauthorized access to a network
2. Weakness in a system that can be exploited by hackers
3. Scamming technique that tricks users into giving personal information

Across: 4. Authentication 5. Malware 6. Encryption Down: 1. Firewall 2. Vulnerability 3. Phishing

DON'T FALL FOR THIS TRAVEL SCAM

Cybercriminals are exploiting travel season by sending fake booking confirmations that look like legitimate e-mails 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

- E-mail 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 travelers often don't double-check e-mails.

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 E-mail Accounts –** Block malicious links and attachments.