

ENDSIGHT.NET

Cybersecurity Office Hours

Stephen Hicks, Security Practice Manager

Q4 2026



endsight



Stephen Hicks
**Security Practice
Manager**
CISSP, CCSP, CISM

Phone Number: (510) 280-2036

Email: shicks@end sight.net



MBA from St. Mary's University.

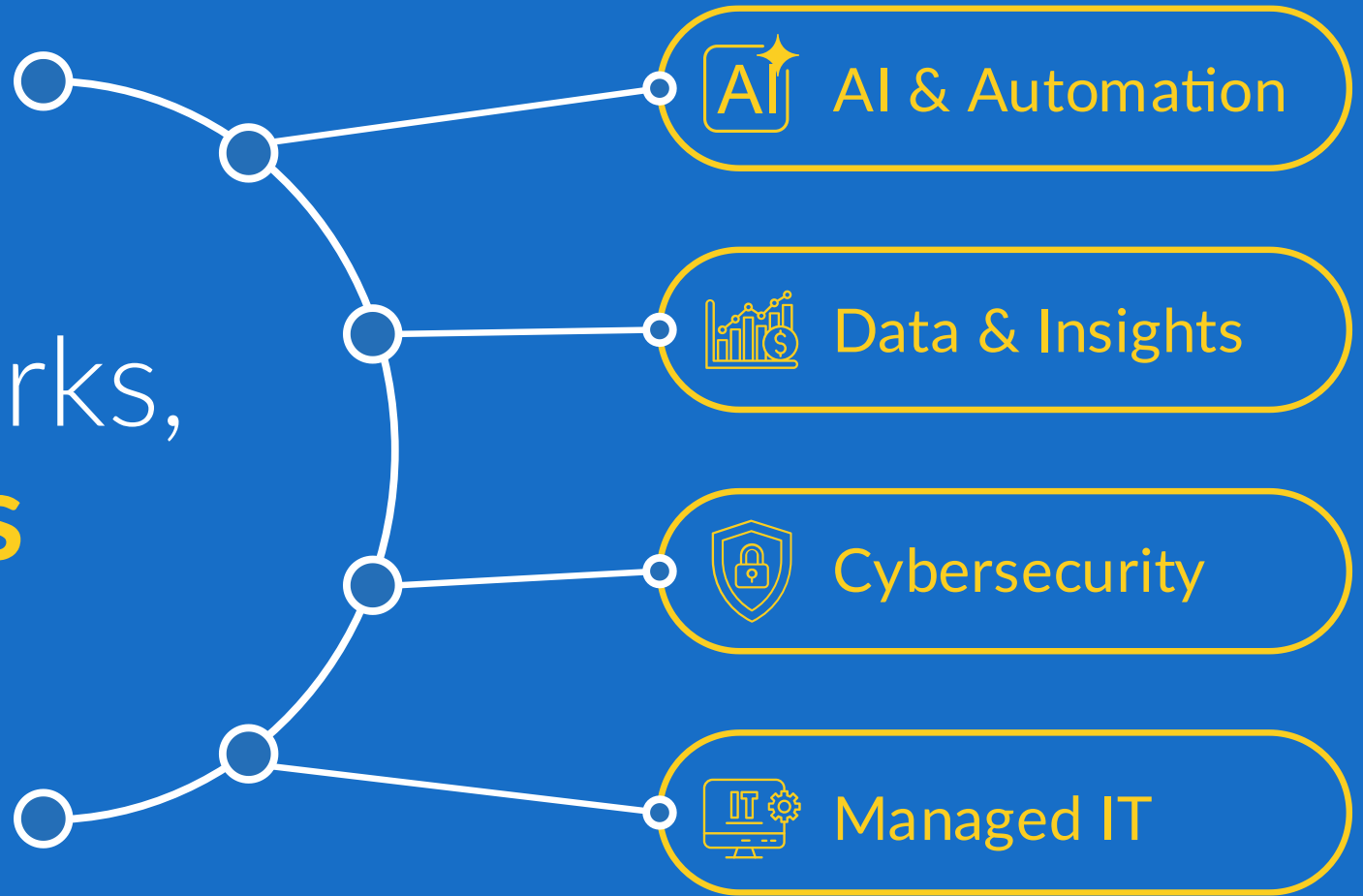


Over 25 years in IT (over a decade in Cybersecurity). Majority of career working with SMBs.

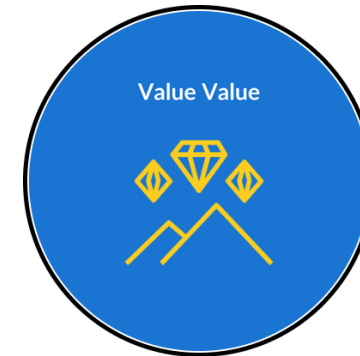
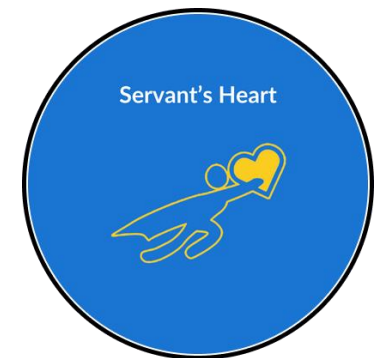
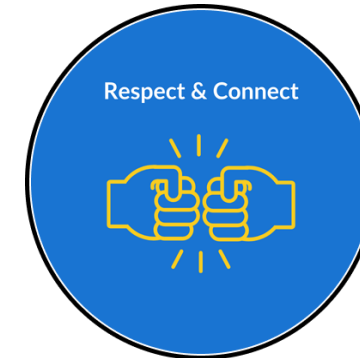
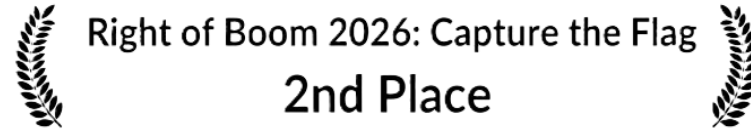


Over a dozen technical certificates.

When your
technology Works,
**Your work gets
easier.**

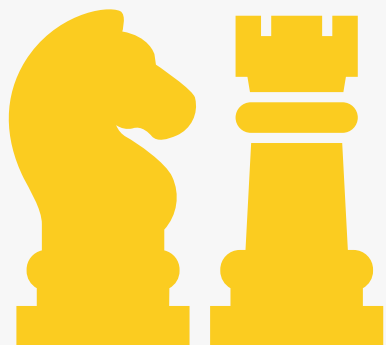


ABOUT



WHAT THIS IS INTENDED TO BE

High level,
strategic discussion



Suitable for
C-Suite



Not tactical,
not user focused



Agenda

01

MATH

02

AI and the Bad Guys

03

PHP and Your Website

04

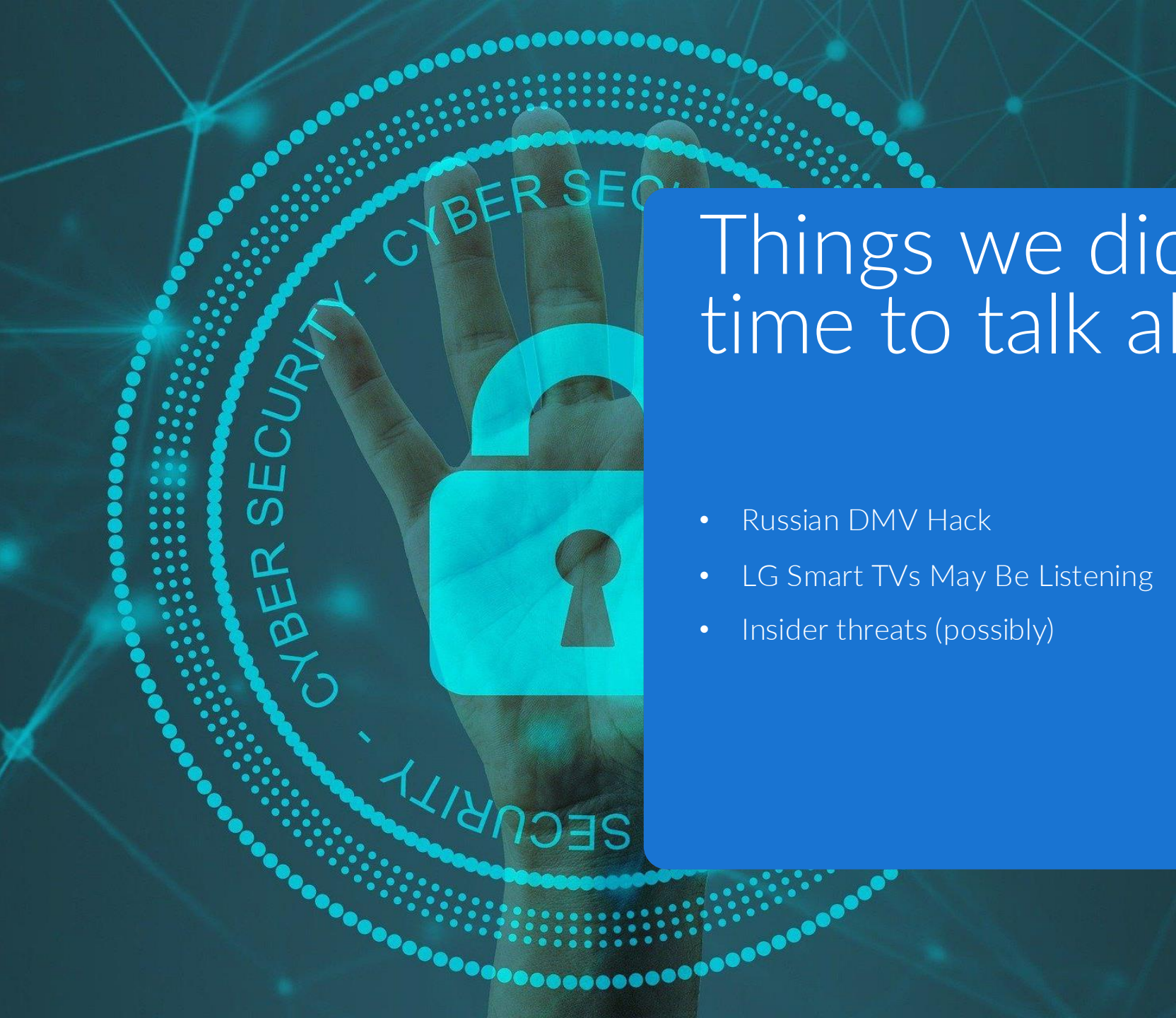
Vendors and Third-Party Risk

05

Insider Threats, Intentional or Not

06

Summary and Q&A



Things we did not have time to talk about

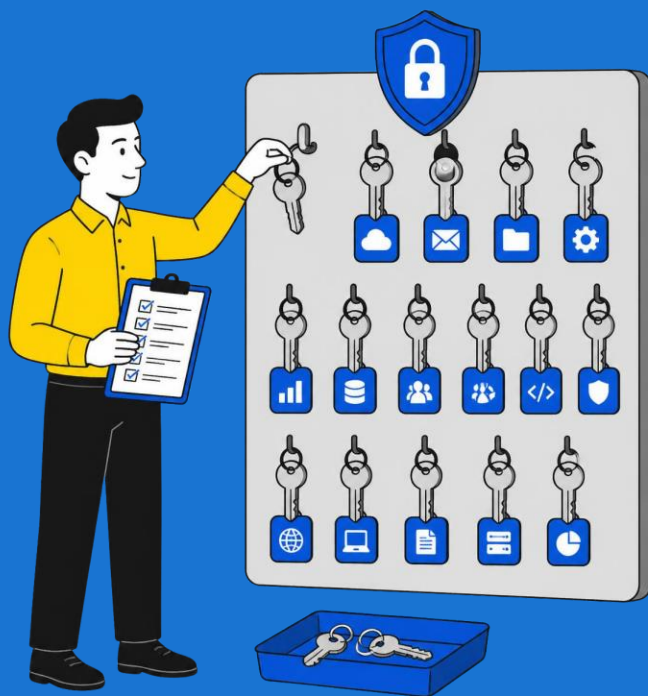
- Russian DMV Hack
- LG Smart TVs May Be Listening
- Insider threats (possibly)

Asymmetric Cryptography



- What are we talking about?
 - Alan Turing and certificates
- What happened?
 - Certificates are the padlock in your browser: proof a website is who it says it is
 - eMudhra, a company that issues them, created 8 with keys anyone could guess in under a second (April 2025)
 - With those keys, an attacker on your network path could fake a padlock for any site, including your bank or Microsoft 365. Modern browsers had an extra check; many apps and devices didn't
 - Reported Oct 17; Google, Mozilla, Apple, and Microsoft blocked them within 3 days
 - No confirmed misuse, but the keys were guessable for about 17 months
 - [bleepingcomputer.com: eMudhra certificates blocked](https://bleepingcomputer.com/news/eMudhra-certificates-blocked/)
 - [blog.cloudflare.com: eMudhra certificate compromise](https://blog.cloudflare.com/eMudhra-certificate-compromise/)
- Why it matters: trust runs through vendors you never chose
 - Your browser updates itself; much of your other software doesn't
 - Apps, remote-access tools, and devices with their own trust lists stay fooled until patched

Checking the Locks



- What Endsight did
 - Opened an incident response Oct 21, the day after Cloudflare's advisory
 - Pushed the Cloudflare fix to all online machines in our management portal; offline machines update when they reconnect, and we follow up on failures
 - Some users may need to sign in again; our support team is ready for those calls
- What to do
 - Update and restart browsers, phones, and computers this week
 - Ask vendors whose software or devices connect to the internet: are you affected, and when will you patch?
 - Never click past a certificate warning or turn off checks to make something work
 - New certificate errors? Call your IT provider (Endsight clients, call us). The fix may be on the vendor's side
- What this means going forward
 - Even the system that proves who's who online has vendors, and they make mistakes
 - Patch speed matters for software you never think about
- What Endsight does about this: EECP monitoring, managed updates on devices we support, and MSSP security reviews

AI and the Bad Guys



- What happened?
 - One extortion crew used an AI coding agent against at least 17 organizations; some ransom demands exceeded \$500,000
 - <https://www.anthropic.com/news/detecting-counteracting-misuse-aug-2025>
 - A state-sponsored group had AI perform 80-90% of a hacking campaign against roughly 30 targets
 - <https://www.anthropic.com/news/disrupting-AI-espionage>
 - FBI: more than 22,000 AI-related complaints in 2025, over \$893 million in losses
 - https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
- The reality check
 - Google has not seen state-backed hackers gain “breakthrough capabilities that fundamentally alter the threat landscape”
 - <https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use>
- Same attacks: cheaper, faster, more of them

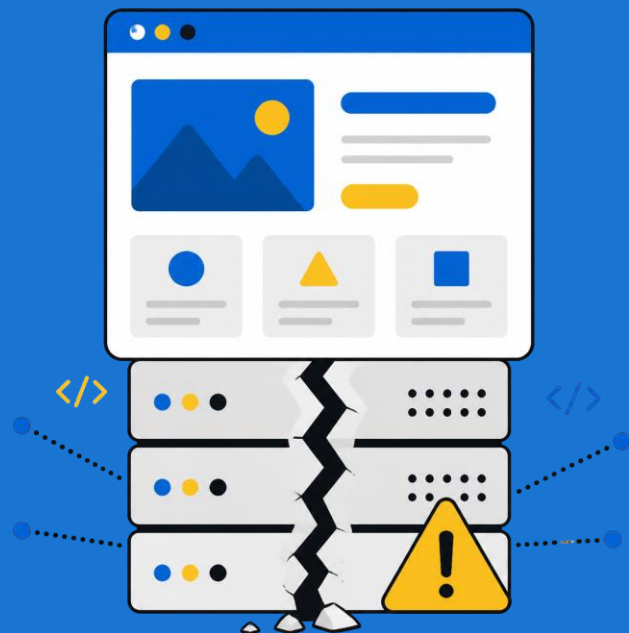
What Changes for SMB?

- Better emails: the typos are gone
 - "Hyper-personalized, culturally nuanced lures" that mirror your company's tone (Google)
- Better recon: who approves payments, who your vendors are
 - AI can "rapidly synthesize" public information to profile targets and map org charts (Google)
- Finding the tiny holes: forgotten logins, exposed keys, loose cloud settings
 - One group scanned 1.8 million mobile apps for passwords and keys left in the code (Anthropic)
- Speed: the window to respond is shrinking
 - Average time from break-in to spreading: 29 minutes; fastest: 27 seconds (CrowdStrike)
- What doesn't change: they still need someone to click, pay, or approve

So What Do We Do About It?

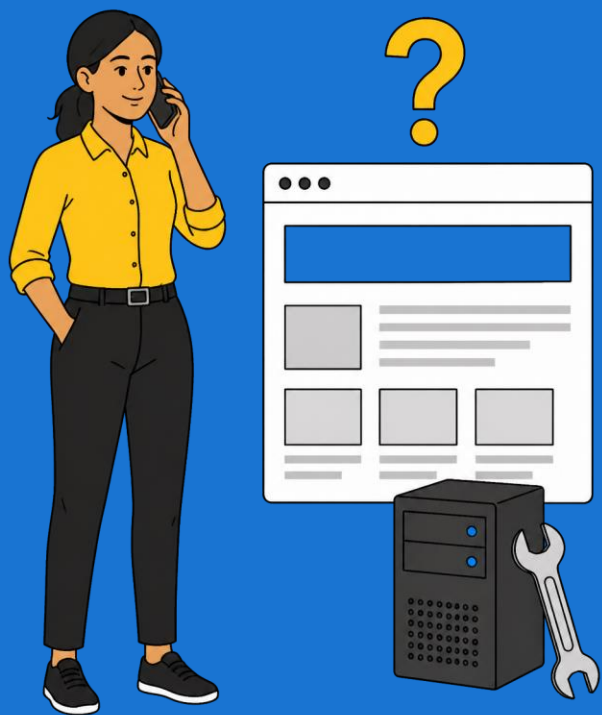
- Defense in depth: no single control stops a well-written lie
 - Verify money and access requests by calling a number you looked up yourself (FBI)
 - Never give a one-time code to anyone who asks for it by email or text (FBI)
 - Code words for payment approvals (yes, again)
- Shrink what AI can find
 - What does your website and LinkedIn say about who approves payments?
 - Old accounts, old vendor access, old cloud settings: who reviews them?
- Plan for minutes, not days: who is watching at 2 AM on a Saturday?
 - What Endsight does about this: EECP detection and response, phish testing and training, and MSSP security reviews
- Which of your processes would survive a perfect email?

The Flaw Under Most Websites



- What happened?
 - PHP is the software behind roughly 70% of websites, including WordPress
 - Oct 20-21: two critical flaws became public. Anyone on the internet can run their own code on an unpatched website's server, no password needed
 - Details leaked **before** the fix; patches shipped Oct 21
 - Attack attempts were seen before the fix existed (Amazon, Oct 17) and continued after it shipped (Cloudflare)
 - cisa.gov: Critical Vulnerabilities in PHP Require Immediate Patching
 - ncsc.gov.uk: Critical security issue affecting PHP
- Why it matters: speed
 - Exploited flaws are now the #1 way attackers get in: 31% of initial intrusions (Verizon DBIR 2026)
 - Endsight sees differently across our clients.
 - Median time to fix a known-exploited flaw: 43 days. Attackers were already trying before the patch existed.

Who Patches a Website?



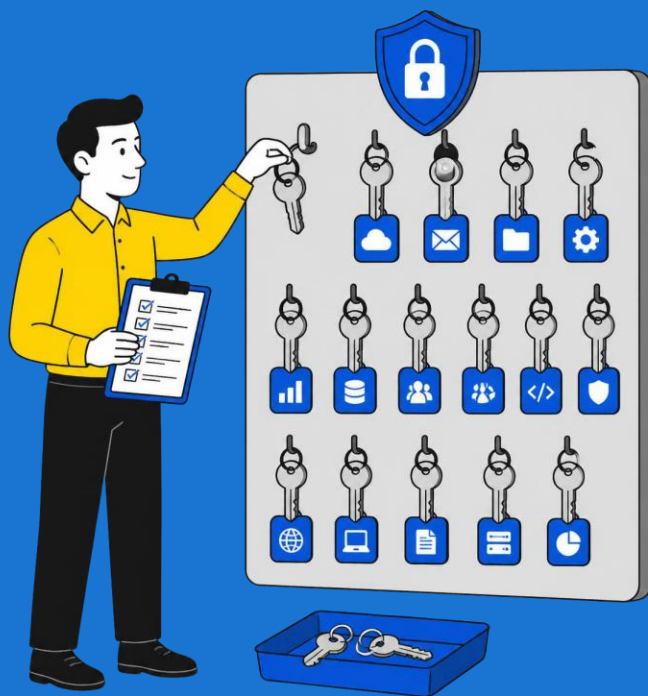
- What Endsight is doing
 - Finding and patching every server that has our management agent and runs PHP
 - Watching every computer with EECPP for signs of attack
- What Endsight can't do
 - We don't host or manage most client websites, and we can't patch servers we don't manage
 - If it doesn't have an Endsight agent, we can't see it. Most hosted websites don't.
- What to do today
 - Call your web developer or hosting provider: do you use PHP, and are you patched?
 - Ask your SaaS and software vendors the same: anything with a built-in web server may run PHP
 - Check devices too: cameras, routers, and other IoT often run a built-in web page
 - Can't patch? Ask about taking it offline (CISA)
- Who is responsible for each of your websites, and would they call you?
- What Endsight does about this: EECPP monitoring, and MSSP recurring security reviews

Vendors and Third Party Risk



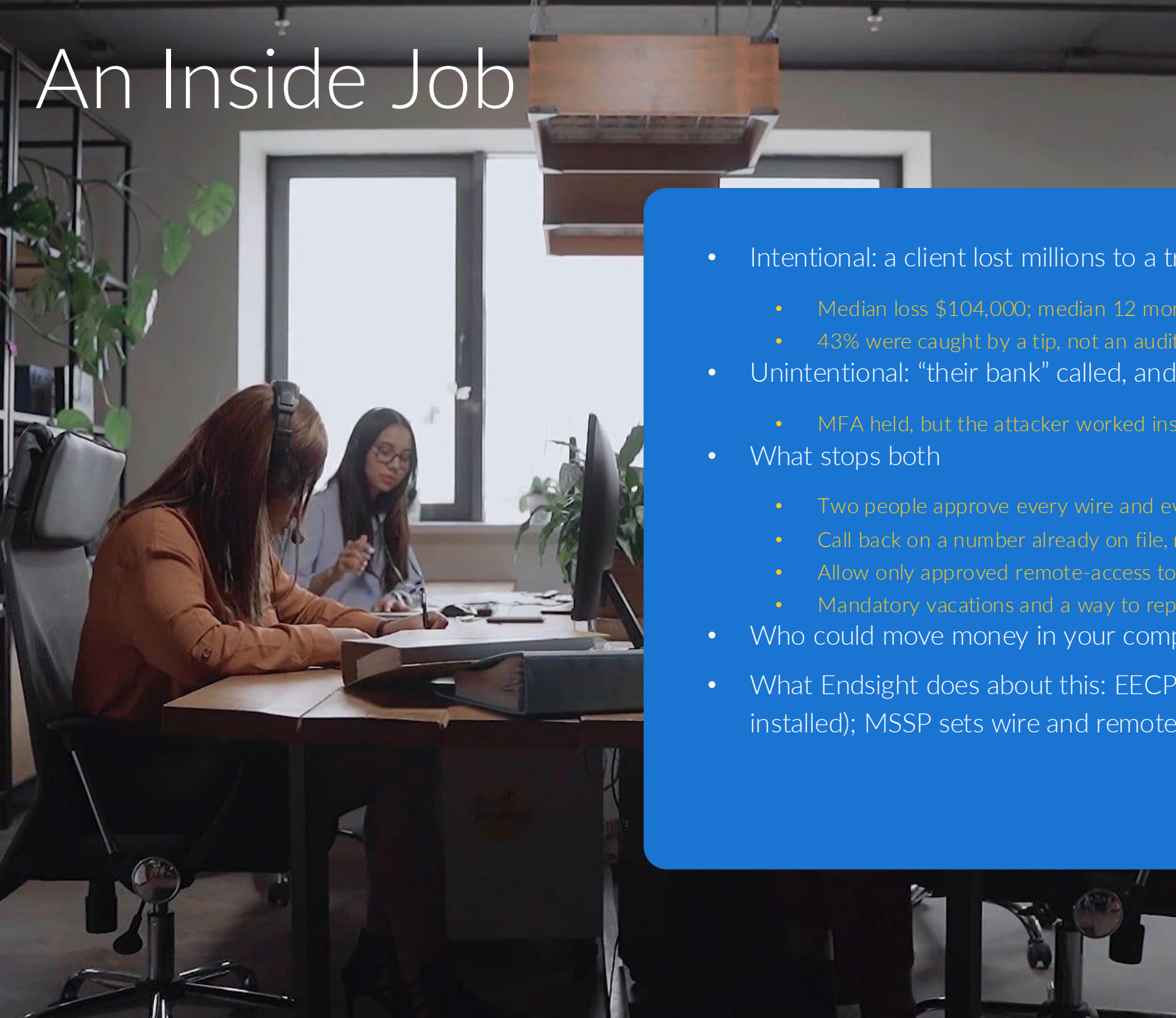
- What happened?
 - An attacker used a stolen credential for ConnectWise Cloud Backup (formerly SkyKick) to sign in to Microsoft 365 as the backup app (Oct 15)
 - Huntress (its customers only): attempts against nearly 1,000 tenants, 162 confirmed compromised
 - ConnectWise suspended the service Oct 17; backups and restores are offline with no restore date
 - [bleepingcomputer.com: ConnectWise supply chain attack](https://bleepingcomputer.com/news/connectwise-supply-chain-attack/)
 - [helpnetsecurity.com: Cloud Backup suspended](https://helpnetsecurity.com/cloud-backup-suspended/)
- Why it matters: third-party risk, again
 - A backup app needs permission to read every mailbox and file; it holds the keys to all of them
 - That access stays in place for years after someone approves it once
 - Third parties were involved in 48% of confirmed breaches, up from 30% (Verizon DBIR 2026)

Who Else Holds Your Keys?



- What Endsight did and continues to do
 - Opened a formal incident response on Oct 16, ahead of public reporting
 - Disabled the ConnectWise apps across the client tenants we manage
 - Reviewed and preserved the logs we hold: no indicators of attacker activity in client tenants; review continues
 - Apps stay off until ConnectWise publishes a verified restoration path
 - Adding alerts for these apps and a connected-app review for new clients
- What to do
 - Inventory the apps connected to Microsoft 365; remove what you don't use (We can help)
 - Ask key vendors about their disclosure policies.
- What this means going forward
 - Attackers now target vendors that hold standing access to many companies at once
 - If you use this product, restores are unavailable until ConnectWise restores service; plan for the gap
- What Endsight does about this: EECP monitoring of Microsoft 365, and MSSP security reviews of connected apps and admin access

An Inside Job

A photograph of two women working at a desk in a modern office. The woman in the foreground is wearing a headset and looking at a computer monitor. The woman behind her is also looking at a monitor. There are plants and a window in the background.

- Intentional: a client lost millions to a trusted insider. No hacker, no malware.
 - Median loss \$104,000; median 12 months before anyone noticed (ACFE 2026)
 - 43% were caught by a tip, not an audit or a tool
- Unintentional: “their bank” called, and an employee installed a remote-access tool
 - MFA held, but the attacker worked inside the employee’s signed-in session
- What stops both
 - Two people approve every wire and every bank-detail change
 - Call back on a number already on file, never one from the call or email
 - Allow only approved remote-access tools; block the rest (CISA)
 - Mandatory vacations and a way to report concerns
- Who could move money in your company without anyone else seeing it?
- What Endsight does about this: EECP watches for remote-access tools (where installed); MSSP sets wire and remote-tool policies

Summary



AI makes old attacks faster



Vendors – certificates, PHP, and risk



Your backup, someone else's keys



Math? Everyone loves math

Summary Continued

People

The single most important piece



Process

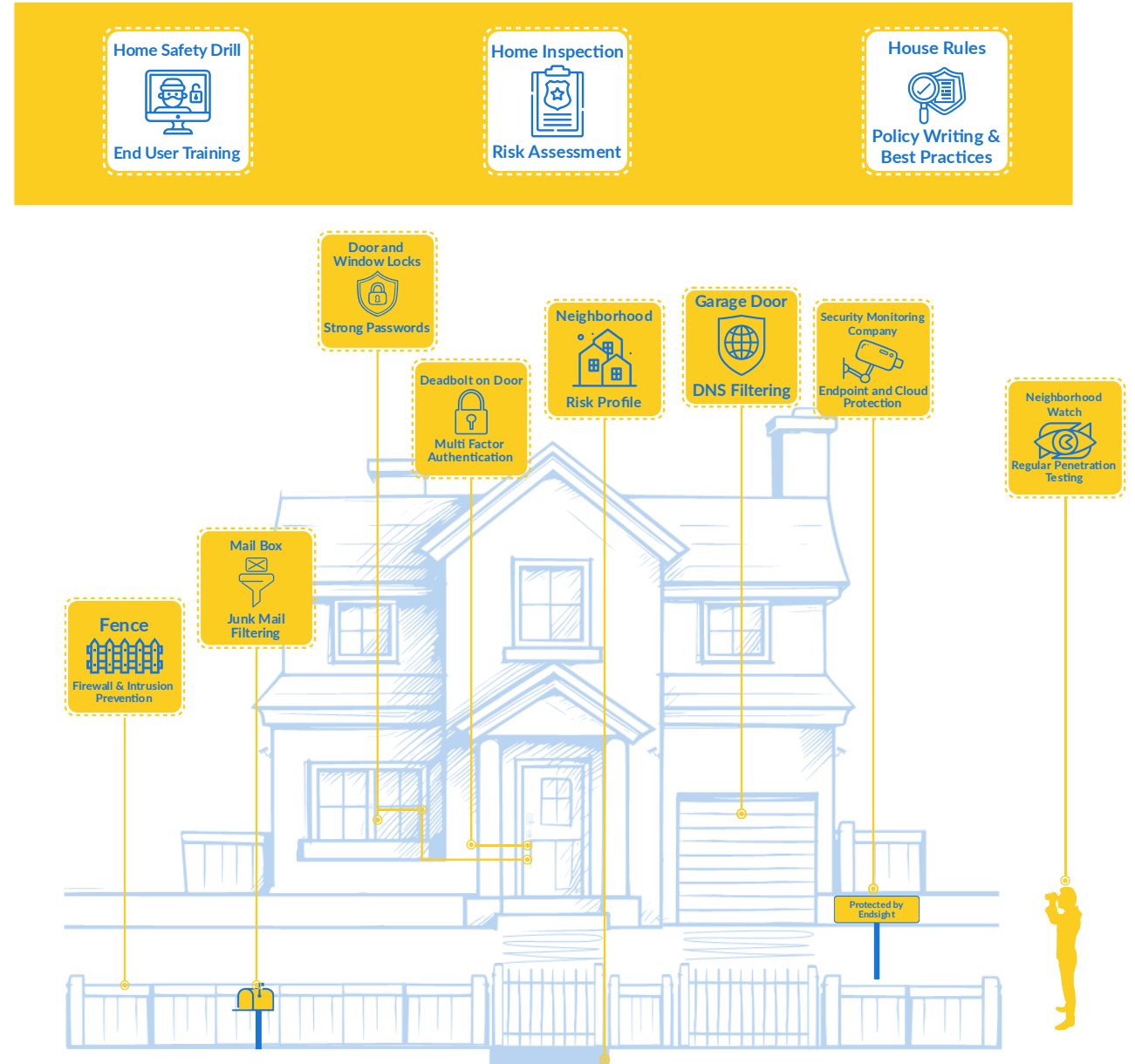


Technology



Defense in Depth

(People, Process, Technology)



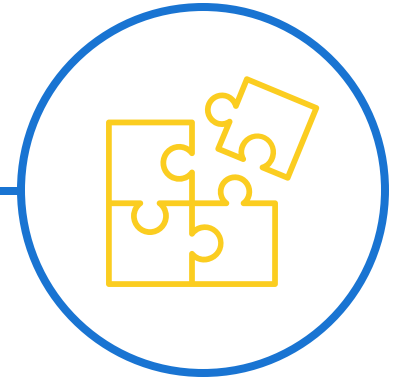
Is Your House in Order?



Contact your Client Strategy Manager or Sales Rep to schedule a call or fill out the form to meet now or later. **Note: If you choose “later,” we’ll reach out in 45 days.**



Take that information to internal stakeholders and see if that's an appropriate risk profile



Work with us to remediate and mitigate the risks

We Hope You'll Join Us Again Soon.

Cybersecurity Office Hours

January 28th

Our next session is January 28th. We hope to see you there!

Register

get.endsight.net/cybersecurity/office/hours



AI Office Hours

November 3rd

A similar format to Cybersecurity Office Hours, focused on AI.

Register

endsight.net/development/webinar



Cybersecurity End-User Training

December 8th

Practical, engaging security training for your whole team, not just IT. Approved for MCLE credit.

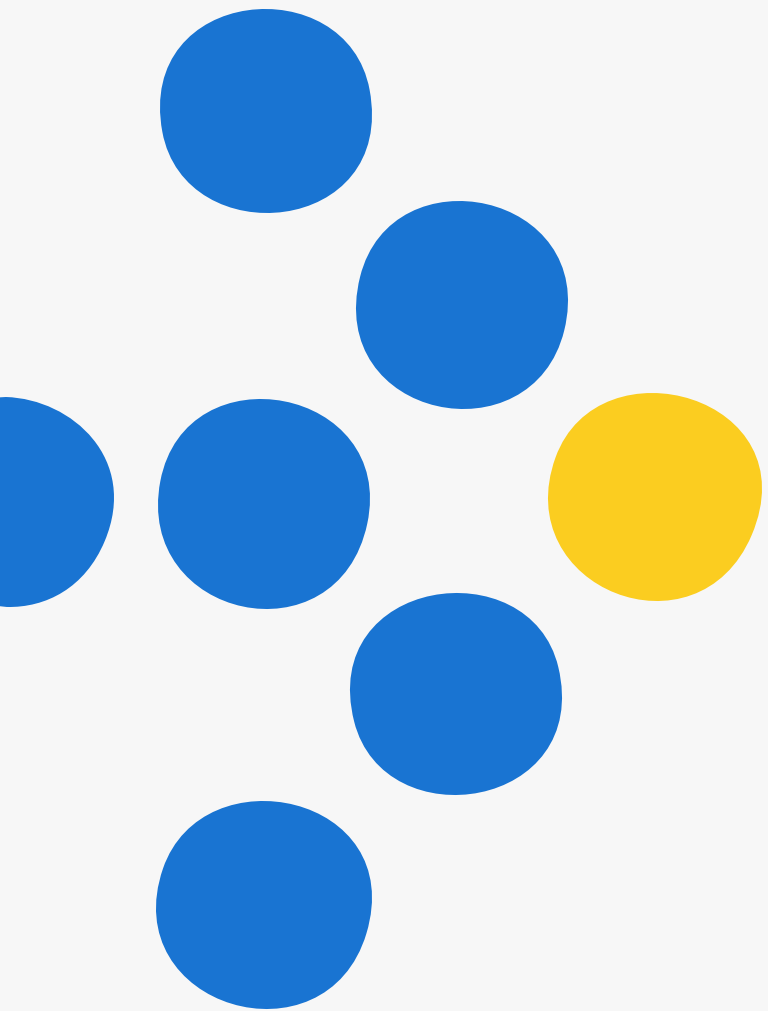
Register

www.endsight.net/cybersecurity-fundamentals-training



To register: fill out the form that's about to pop up, or email akreps@endsight.net asking to register. For Cybersecurity Office Hours, we can auto-register you for every session in 2027.

We'd love to hear from you. A short survey is on its way. Your feedback shapes what we cover next.



Q&A



Q&A

- How can you tell you've been compromised? For example, a slower computer or glitches?
- How should I be thinking about data privacy when using AI tools?
- What are silent threats, and how can I tell if one is already in my environment?
- I work from home. Are my servers protected?
- What's going on with the PHP issue, and what are the points of most concern?
- What happened, and did the white hat who found the loophole give the security side enough of a head start on the malicious actors?
- What do we need to watch out for with SkyKick and PHP? And what's the deal with the ConnectWise compromise?



Stephen Hicks
CISSP, CCSP, CISM
Security Practice Manager
@Endsight

Thank
you!