ENDSIGHT.NET

Cybersecurity **Office Hours**

Stephen Hicks, Security Practice Manager

Q1 2026

endsight

Stephen Hicks

Security Practice Manager

CISSP, CCSP, CISM

Phone Number: (510) 280-2036
Email: shicks@endsight.net

MBA from St. Mary's University.

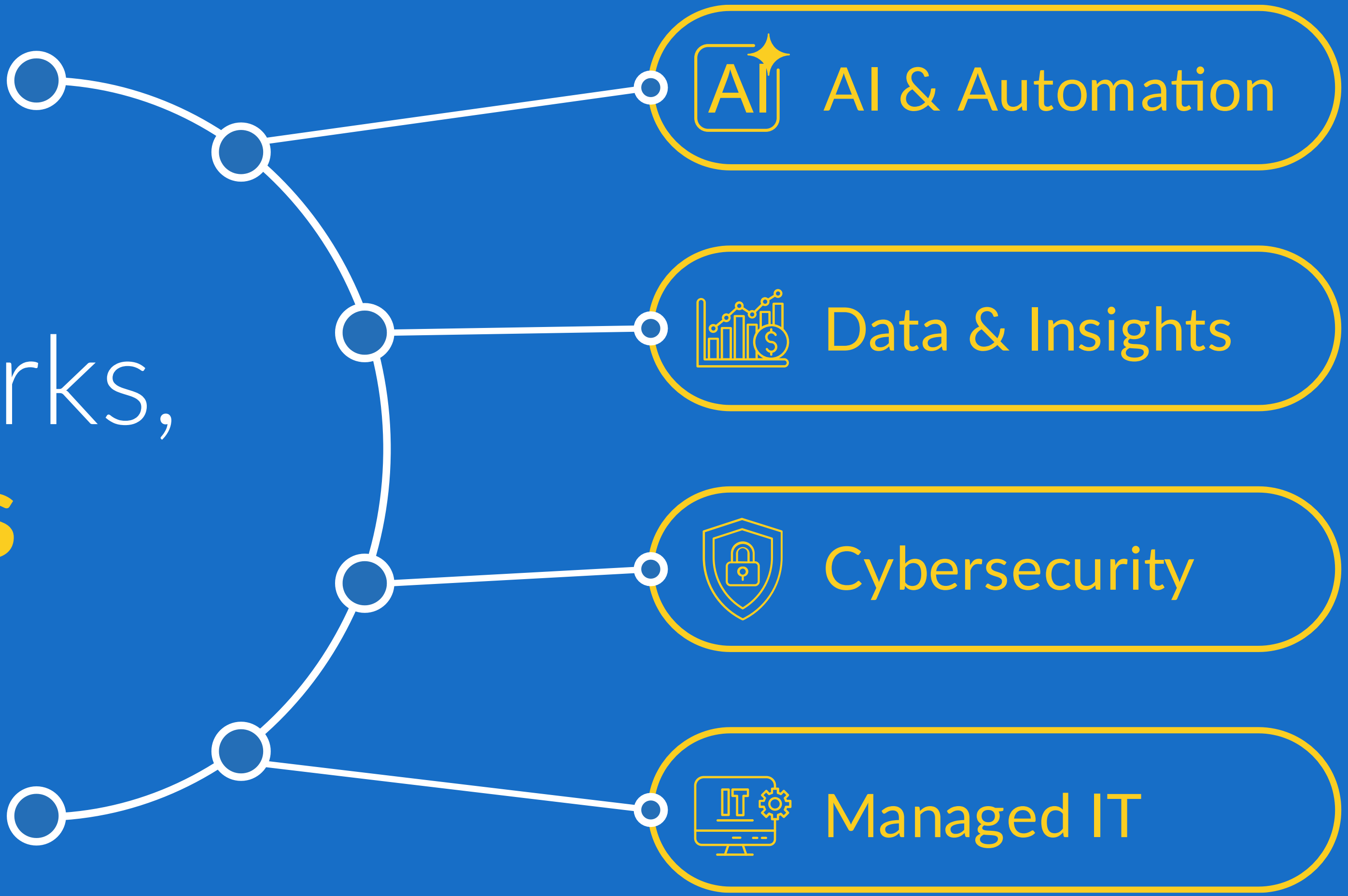
Over 25 years in IT (over a decade in Cybersecurity).
Majority of career working with SMBs.

Over a dozen technical certificates.

> We live in the darkness, so you don't have to. ”

When your technology Works,

Your work gets easier.



AI & Automation

Data & Insights

Cybersecurity

Managed IT

endsight

Purpose: Help others thrive

MSP 501
Channel Futures 2025

San Diego Business Journal
2025 TOP
TECHNOLOGY SOLUTION PROVIDERS

Right of Boom 2025: Capture the Flag
2nd Place

THE CHANNEL CO.
CRN
FAST GROWTH 150
2025

THE CHANNEL CO.
CRN
SOLUTION PROVIDER 500
2025

Respect & Connect

Servant's Heart

Value Value

Progress Over Comfort

What Security Office Hours is intended to be

High level, strategic discussion

Suitable for **C-Suite**

Not tactical, not user focused

Agenda

01 What is HIBP?

02 AI espionage and malicious tools

03 How did the AI attack work?

04 AI in compromised accounts

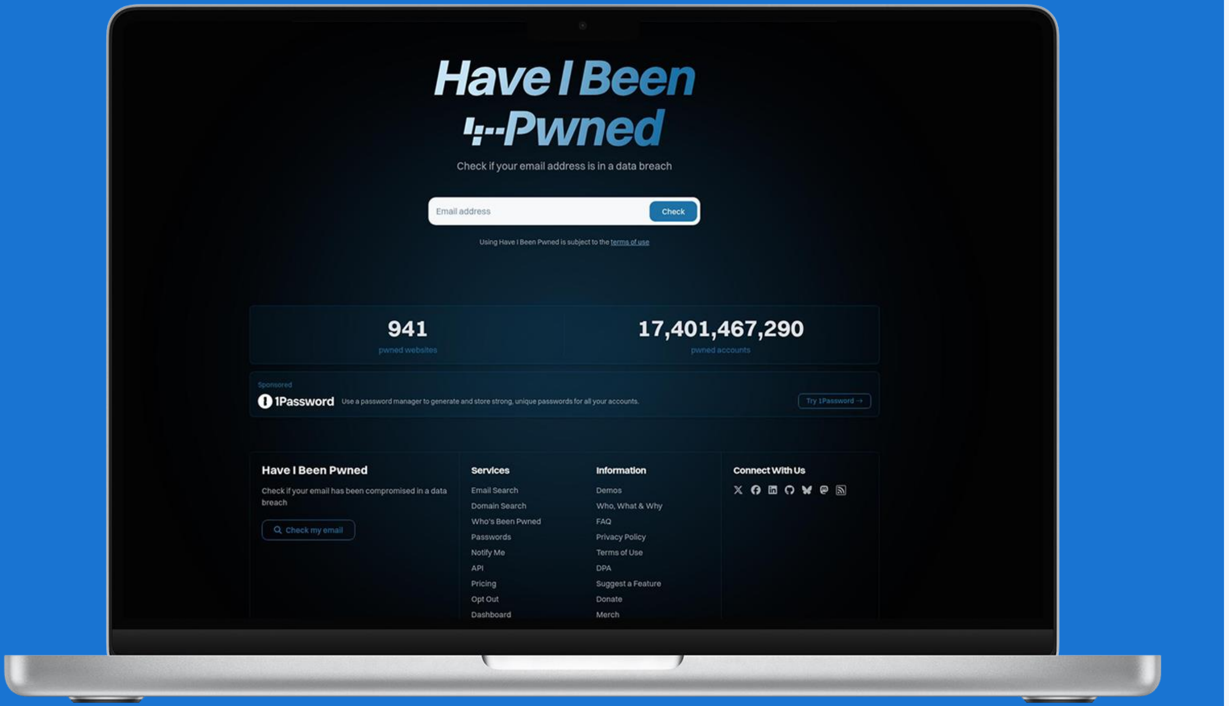
05 Emerging threat – Apps and AI in Teams calls

06 Restricting applications in calls

07 Summary

08 Q&A

What is HIBP?



Have I Been Pwned

Check if your email address is in a data breach

Using Have I Been Pwned is subject to the terms of use

941 pwned websites

17,401,467,290 pwned accounts

Sponsored

1Password Use a password manager to generate and store strong, unique passwords for all your accounts.

Have I Been Pwned

Check if your email has been compromised in a data breach

- Have I Been Pwned (Owned) is one of largest database of compromised passwords
- Searchable database of addresses with related information
- Recent major additions:
  - Synthient (1.96 *Billion* accounts)
  - WIRED (2.4 million accounts)
  - Allianz Life (1.1 million accounts)
- The Dark Web – why it's important, but also isn't important.

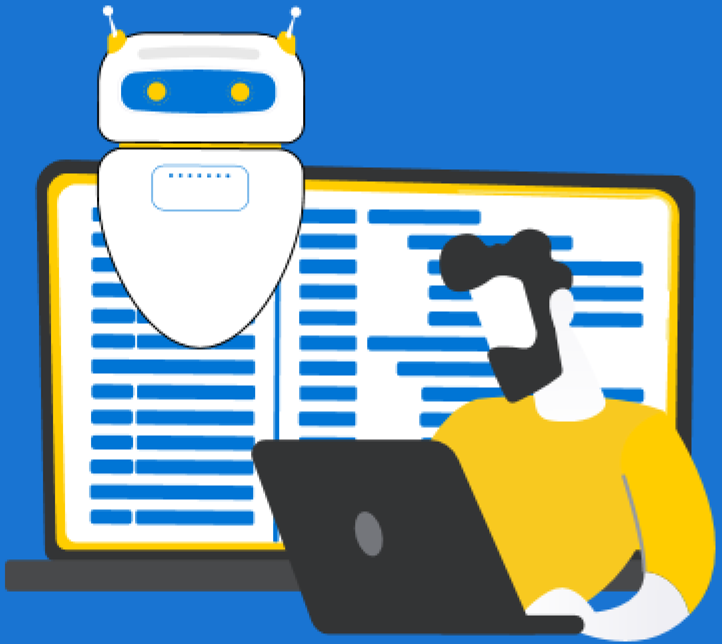
AI espionage and malicious tools

Anthropic (Claude) has declared an inflection point where AI is both good and bad for security and is now at least effective.

Anthropic has started finding (and disrupting) AI based attacks:

- AI to create the malicious code
- AI agents to attempt cyberattacks and execute payloads
- Humans to review the AI, but none of the work

https://www.anthropic.com/news/disrupting-AI-espionage



What does this mean?

- Faster code revision
- Stronger, faster attacks
- Increased attack points (AI can test multiple points of ingress simultaneously)

How did the AI attack work?

- Human operator provides targets
- AI scans for target accessibility and analyzes publicly available code/endpoints.
    - Human reviews results.
- AI scans targets for vulnerabilities and attempts exploits (automatically)
    - Human reviews results and directs further action.
- AI uses exploits to perform *internal* recon and validates data access.
- AI automatically exfiltrates data
- https://www.anthropic.com/news/disrupting-AI-espionage

AI in compromised accounts

The stages of the attack lifecycle:

- Recon
- Breach
- Recon
- Payload

Where does AI fit in here?

- Recon speed
- Automatic exfiltration

What do we do about this?

endsight

Restricting applications in Microsoft Teams calls

Only Microsoft Products
Only Microsoft Products + Third Party Approval
No Applications Allowed
All Applications Allowed

- Endsight's security team is currently investigating limiting application access in Teams. Potential approaches:
  - Only Microsoft products
  - Only Microsoft products with a process to approve third party
  - No applications allowed
  - All applications allowed
- This is particularly relevant to legal, where AI notetakers can *cause a loss of attorney client privilege*
  - The Silent Guest in Your Meetings: Legal Risks of AI "Note-Takers"
- Additional information to follow

Summary

This summary not written by AI

Have I Been Pwned and the Dark Web

AI attacks and scalability

Apps and AI in video calls

Summary Continued

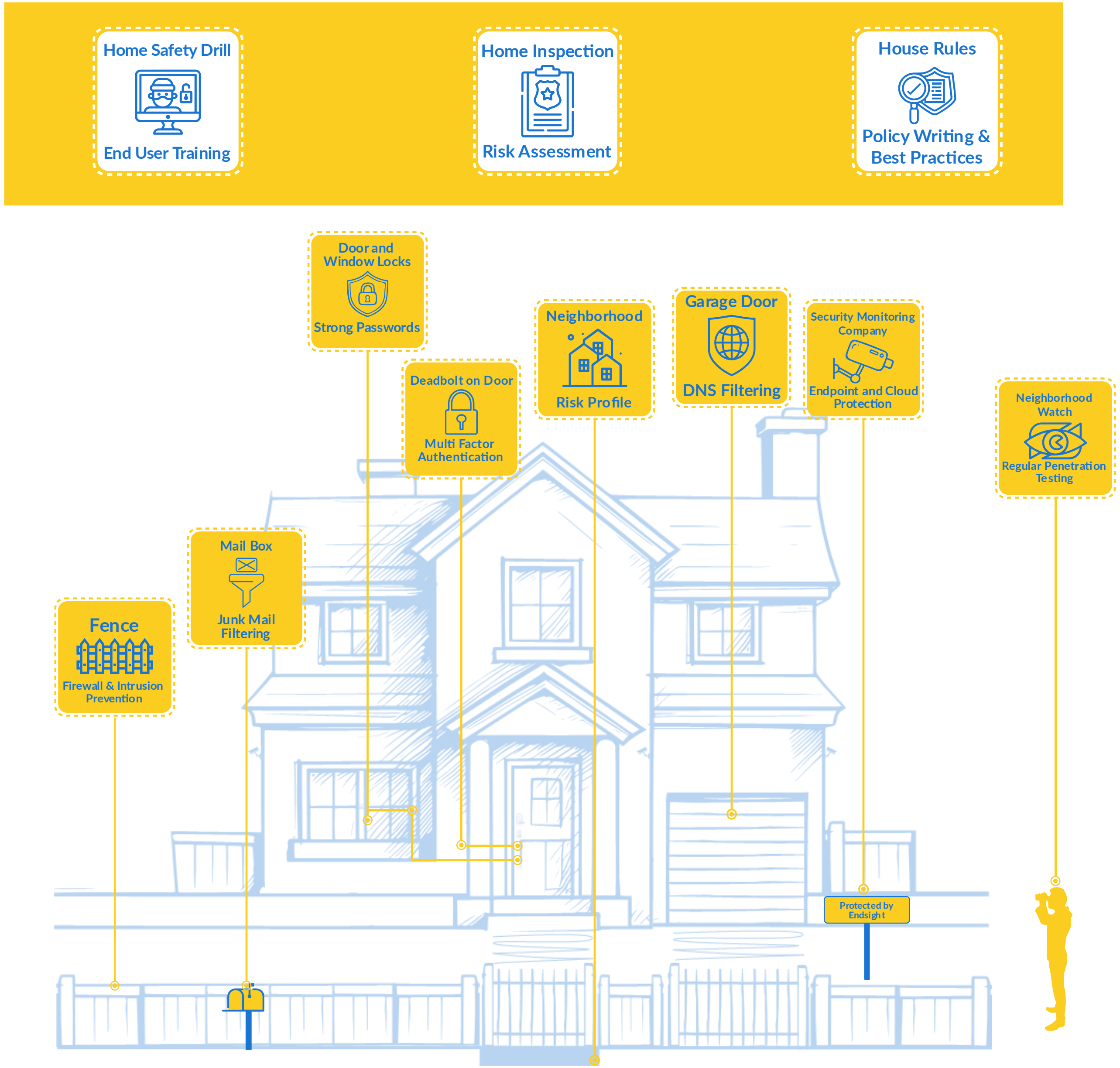
People
The single most important piece

Process
What to do and how to do it

Technology
Always required

Defense in Depth

(People, Process, Technology)



Home Safety Drill
End User Training

Home Inspection
Risk Assessment

House Rules
Policy Writing & Best Practices

Door and Window Locks
Strong Passwords

Deadbolt on Door
Multi Factor Authentication

Neighborhood
Risk Profile

Garage Door
DNS Filtering

Security Monitoring Company
Endpoint and Cloud Protection

Neighborhood Watch
Regular Penetration Testing

Mail Box
Junk Mail Filtering

Fence
Firewall & Intrusion Prevention

Protected by Endsight

How Protected are you from **Cyber threats?**

Most business leaders overestimate their cybersecurity maturity because no one has ever given them a clear way to measure it .

Take our self-assessment to, get a clear picture of where you stand and a starting point to strengthen your defense

Is your house in order?

Our 10-minute self assessment can help you determine where you stand and what to do next

1

Reactive

Unplanned. Unprotected. Unaware of what you don't know.

2

Aware

Some defenses. Thin strategy. This is where most businesses get stuck.

MOST BUSINESSES ARE HERE

3

Defined

Intentional. Budgeted. You can survive an incident.

4

Proactive

Security is part of how you operate, not an afterthought.

5

Strategic

Security drives trust, sales, and growth.

Most Businesses Land at Level 2. Where Do You Fall?

Scan. Score. See Where You Stand.

www.endsight.net/security

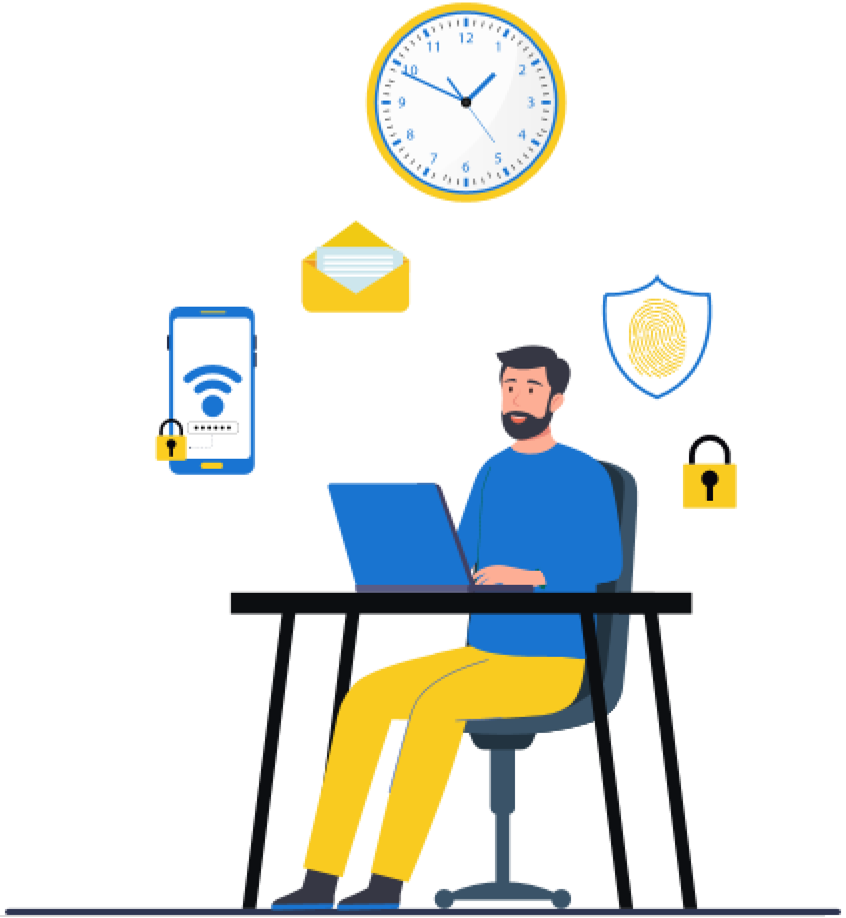
Scan Me

endsight

Next Session

April 30th @ 1 PM PST.

- To register:
  - Scan the barcode
  - Go to: https://get.endsight.net/cybersecurity/office/hours
  - Email akreps@endsight.net to register
    - We can register you for the next one.
    - To register for all of the remaining 2026 sessions, please email akreps@endsight.net

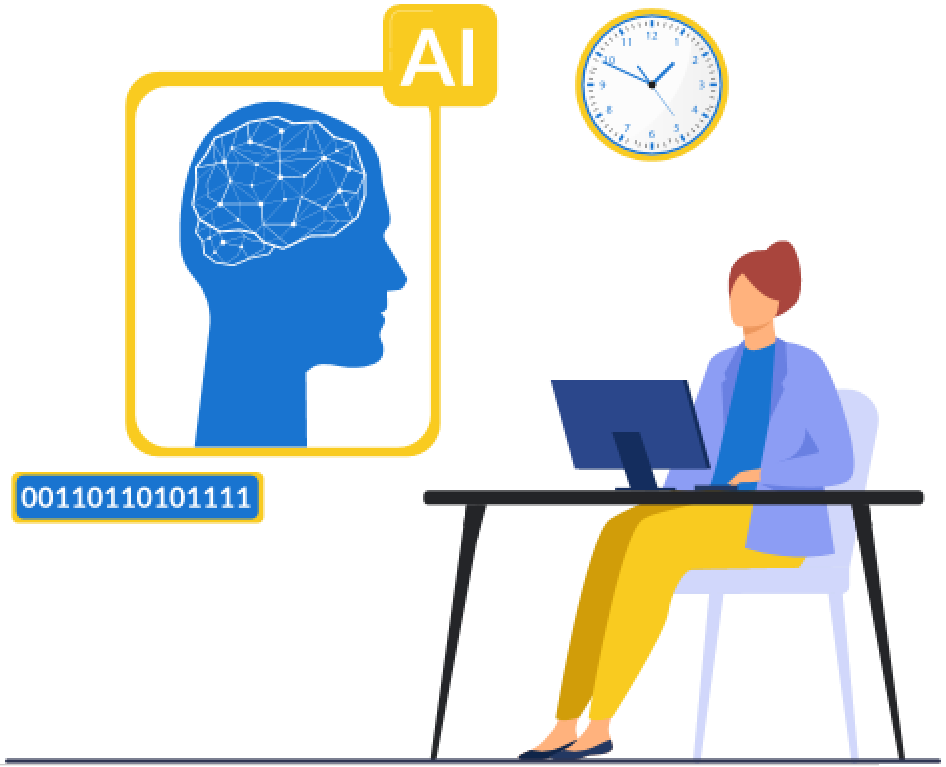


AI Office Hours

March 5th @ 1 PM PST.

Similar format to Security Office Hours, but AI focused.

- To register:
  - Scan the barcode
  - Go to: https://www.endsight.net/development/webinar
  - Email akreps@endsight.net to register



Q&A

Q&A

- What advice do you have for managing third-party SAAS providers for AI use either in products purchased or internally that could impact confidential data?
- How can organizations protect customer records and CRM-connected applications, such as Commerce7 checkout portals that collect credit card information, from bad actors posing as legitimate customers and placing fraudulent orders?
- What ongoing steps should organizations take, on a yearly and monthly basis, to keep unauthorized users out of their systems?
- Is MS Teams Chat being used in place of email for targeted phishing? What can my organization do to lock down MS Teams?

Q&A

- I’ve seen news stories about AI cloning people's voices perfectly. Honestly, if my finance manager gets a call that sounds exactly like me asking for a wire transfer, how are they supposed to know it's fake? Does Endsight have protocols to help us spot these deepfakes?
- It sounds like the old 'Prince of Nigeria' emails are being replaced by hyper-personalized AI messages that know everything about us. How can we protect ourselves as this evolves?
- This might be a few years out, but I hear people talking about 'Quantum computing' breaking all current security encryption. Is that something we need to worry about now?

Stephen Hicks

CISSP, CCSP, CISM

Security Practice Manager

@Endsight

Thank you!

endsight