CYBERSECURITY OFFICE HOURS

endsight

www.endsight.net | info@endsight.net | (833) 363-7444

endsight

About Stephen Hicks

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

- Over 25 years in IT (over a decade in cybersecurity).
- Over a dozen technical certifications
- MBA from Saint Mary's college
- Majority of career working with SMBs

☎ (510) 280-2036

✉ shicks@endsight.net

ABOUT

San Diego Business Journal
2024 TOP
TECHNOLOGY SOLUTION PROVIDERS

MSP 501
Channel Futures 2024

THE CHANNEL CO.
CRN
SOLUTION PROVIDER 500
2024

SAN FRANCISCO BUSINESS TIMES
2024 BEST PLACES TO WORK IN THE BAY AREA
2024 BEST
PLACES TO WORK
B P t W
Endsight
RANKED #24

THE CHANNEL CO.
CRN
FAST GROWTH 150
2024

Inc. 5000
9 time honoree 2024

Respect & Connect

Servant's Heart

Value Value

Progress Over Comfort

endsight

WHAT THIS IS INTENDED TO BE

- High level, strategic discussion
- Suitable for C-Suite
- Not tactical, not user focused

Trends and Events in the last quarter

endsight

Trends, Continued

endsight

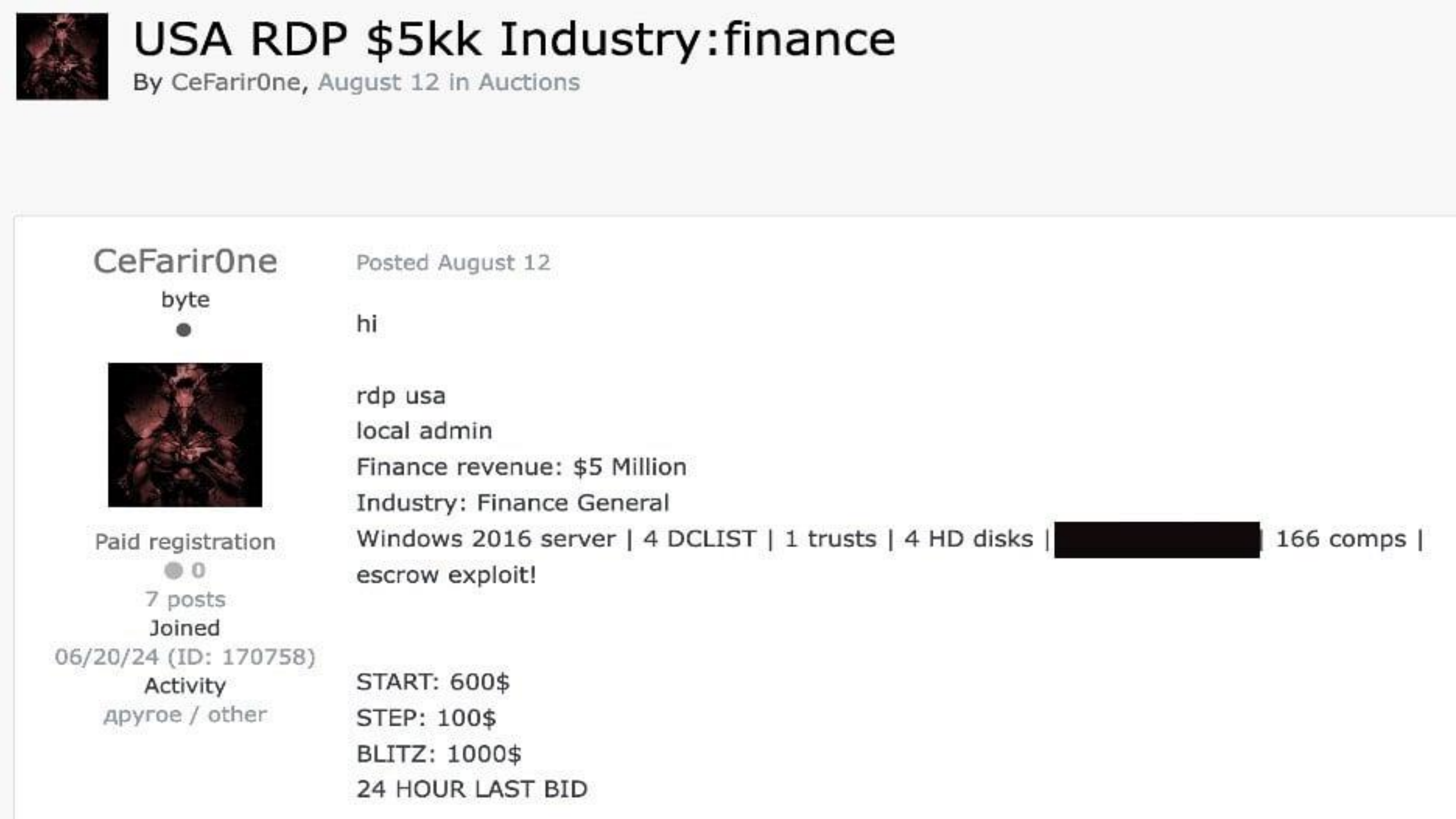
Lifecycle of an Attack

From Phish to $2.5M Ransomware Attack

START

An employee clicked a link in a phishing email. This enabled the attackers to get the access credentials for the Domain Admin.

SOPHOS
Cybersecurity evolved.



USA RDP $5kk Industry:finance

By CeFarir0ne, August 12 in Auctions

CeFarir0ne
byte
●

Paid registration
● 0
7 posts
Joined
06/20/24 (ID: 170758)
Activity
другое / other

Posted August 12

hi

rdp usa
local admin
Finance revenue: $5 Million
Industry: Finance General
Windows 2016 server | 4 DCLIST | 1 trusts | 4 HD disks | [redacted] | 166 comps |
escrow exploit!

START: 600$
STEP: 100$
BLITZ: 1000$
24 HOUR LAST BID

AI driven phishing attacks

- Allows for far better email.
- Can scrape information from public sources (LinkedIn, Facebook, Instagram, Twitter).
- Allows for more frequent and targeted phishing (75% increase from last year).
- What to do about it?

endsight

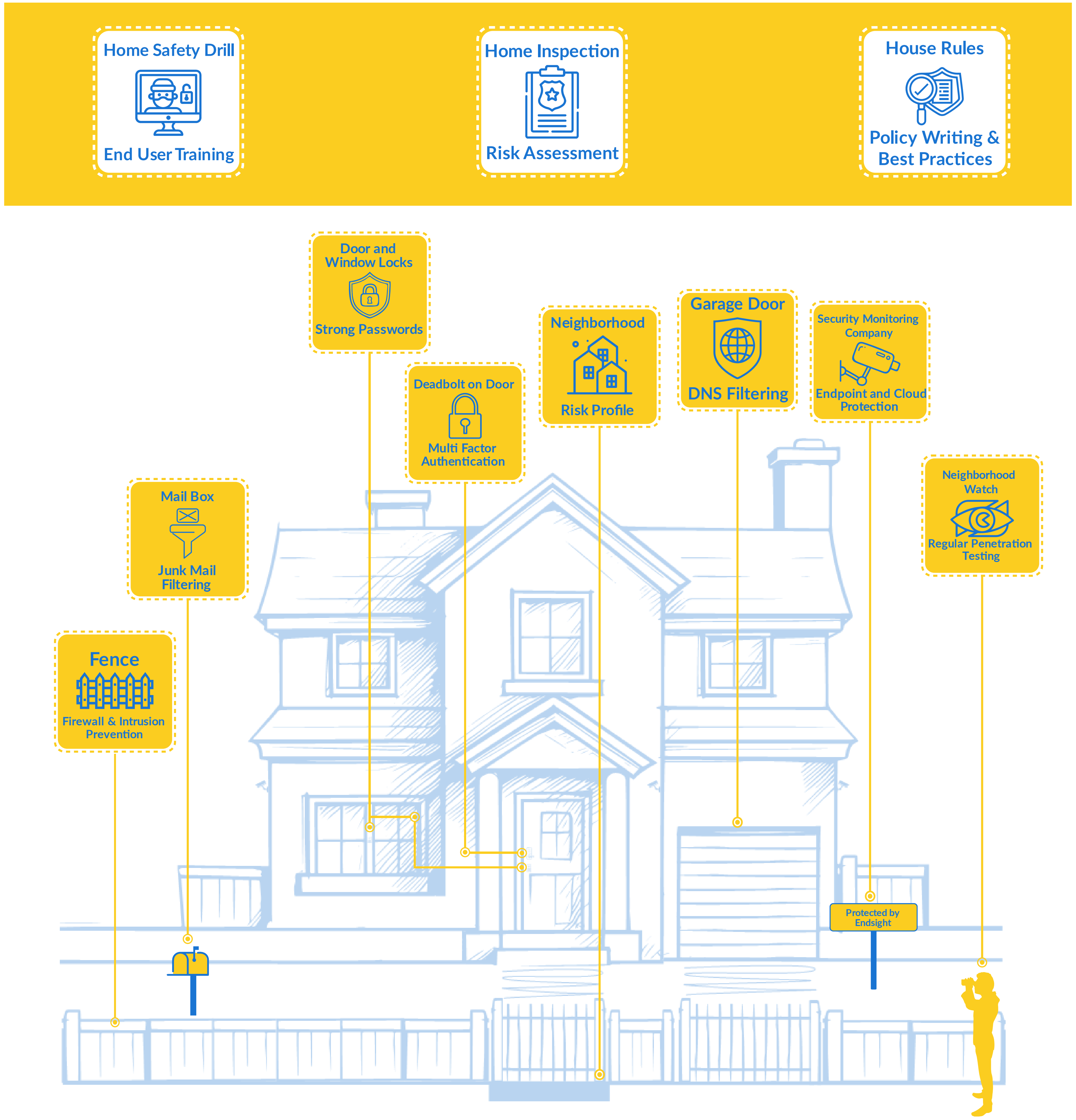
Phishing Defense

- Phishing defense (and all cybersecurity) is people, process, and technology *in that order.*
- Training, policy writing, and technical solutions.
- All three pillars are important, but one is most interesting…

endsight

Layered Cyber Security

(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

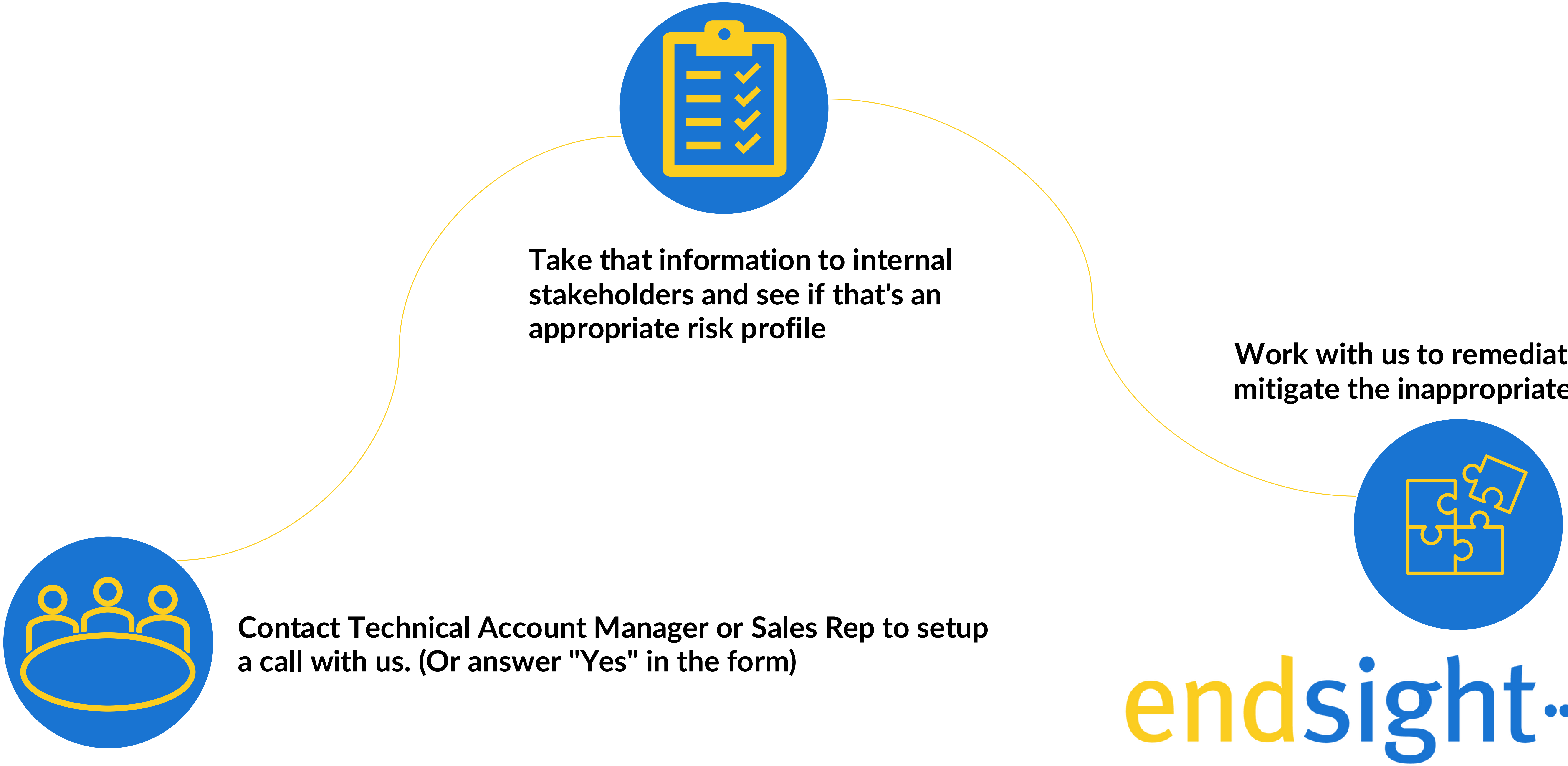
Security Monitoring Company
Endpoint and Cloud Protection

Neighborhood Watch
Regular Penetration Testing

Mail Box
Junk Mail Filtering

Fence
Firewall & Intrusion Prevention

Is Your House in Order?



Contact Technical Account Manager or Sales Rep to setup a call with us. (Or answer "Yes" in the form)

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

Work with us to remediate and mitigate the inappropriate risks

endsight

SUMMARY

1. People, process, and technology (in that order)
2. Size of organization is irrelevant. No longer human driven attacks, but human driven exploits
3. Data is cheaply for sale
4. Users are on the attackers' side, and they don't even know it.
5. Continual audits and reviews are the most effective, least expensive security solution.

Q&A

- How to handle Microsoft 365 issues with emails getting impersonated by other people. Our organization uses 1password but recently, we've had issues with emails getting hacked. There was a particular incident where a faulty link impacted the Microsoft two-authenticator system and allowed an email to be hacked. Any practical tips are appreciated!
- Is cybersecurity insurance worth it? If Endsight was running/managing our IT, would we still need cyber insurance?
- What's the best way to keep employees aware of what they can / need to do as part of their role in Enterprise Risk Management as a whole, and Cybersecurity as part of that.
- How important is using a VPN for general use offsite and when not logging into a domain/remote desktop at work.

endsight

UPCOMING SESSIONS

- Want us to auto register you for our 2025 sessions?

- Next session will be on February 13th, but if you answer "Yes," in the form, we'll auto register you for every 2025 Office Hours sessions! The remaining 2025 sessions are TBD.

- Next Topic: Top Threats Endsight saw in 2024.

endsight

endsight

Thank you!

☎ (510) 280-2036

✉ shicks@endsight.net

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