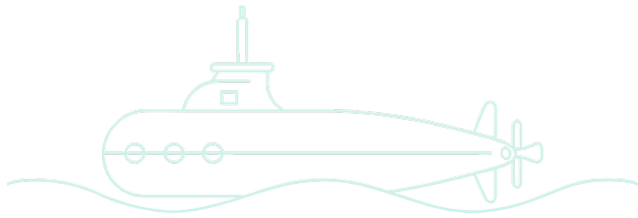
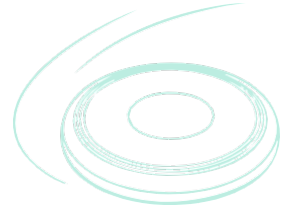


WELCOME!



Community Health Center Association of Connecticut

**To claim CMEs for this session
please scan the QR code to log
attendance and complete the
required survey.**



Cybersecurity & Patient Data: Innovations in Protecting Sensitive Health Information



Jeff Olejnik
Partner – CyberTech
WIPFLI



CHC/ACT

Community Health Center
Association of Connecticut

THRIVE

The background of the slide features a photograph of a healthcare professional, likely a doctor, wearing a white lab coat and glasses, smiling while examining a baby. The baby is being held by a woman. A stethoscope is visible around the doctor's neck. In the foreground, a hand is holding a blue medical ID badge with a signature and the name 'S. G. ...' written on it. The word 'THRIVE' is overlaid in large, white, bold, sans-serif capital letters across the center of the image.

Cybersecurity & Patient Data: Protecting
Sensitive Health Information

WIPFLI

Agenda

Cybersecurity Threat Landscape

Anatomy of an Attack

Baseline Security Controls

Innovative Controls for safeguarding ePHI

Leadership and Board Oversight



Today's Threat Landscape

Rising Cyberattacks in Healthcare

Over 400 HC organizations faced cyberattacks in 2024

Major Data Breaches

Change Healthcare attack exposed PHI of 259 million Americans

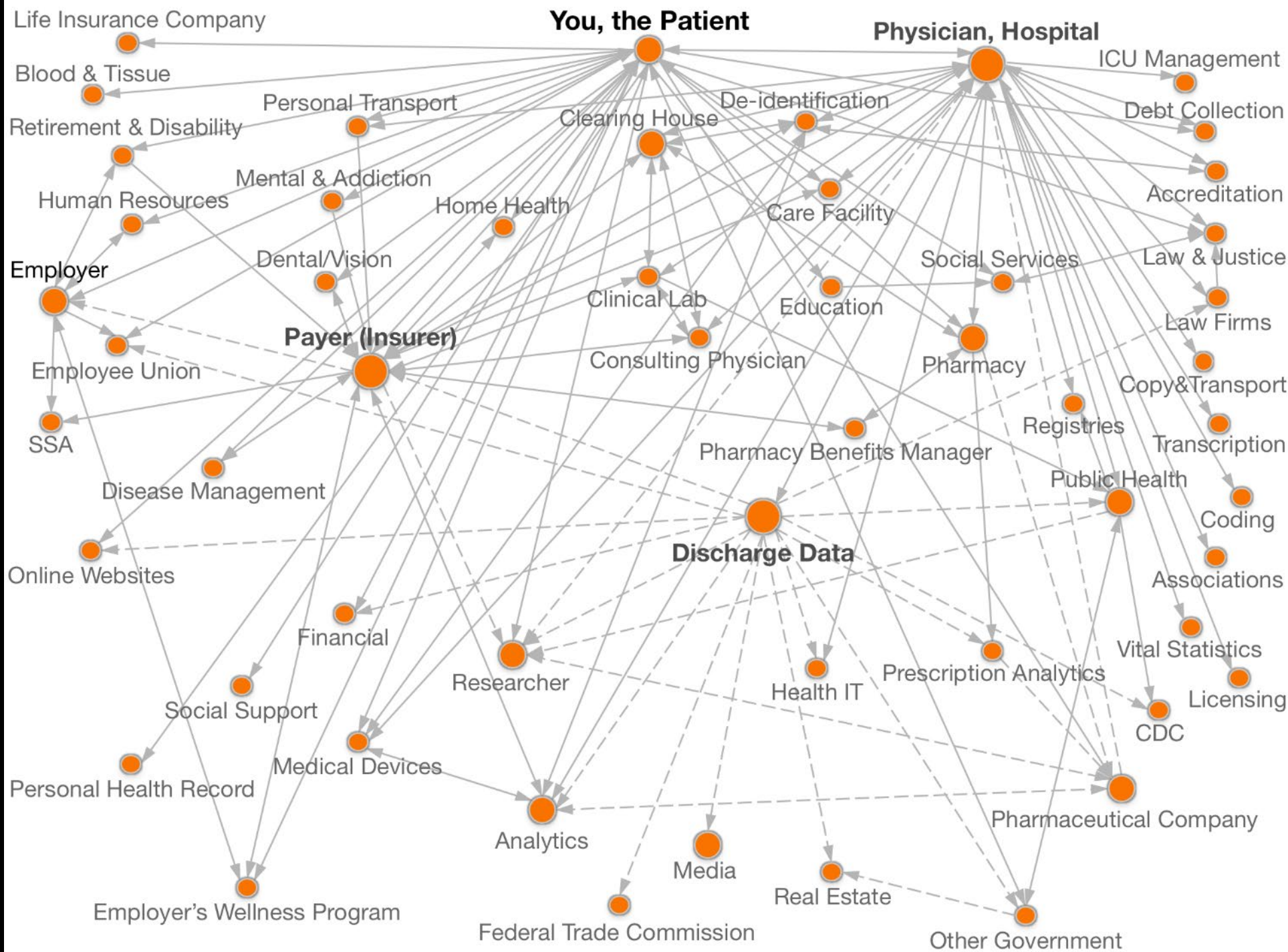
Supply Chain Vulnerabilities

80% of breaches stem from third-party vendors

Expanded Attack Surface

AI, cloud, and IoMT integration widen cyberattack opportunities in healthcare systems

Attack surface is huge!



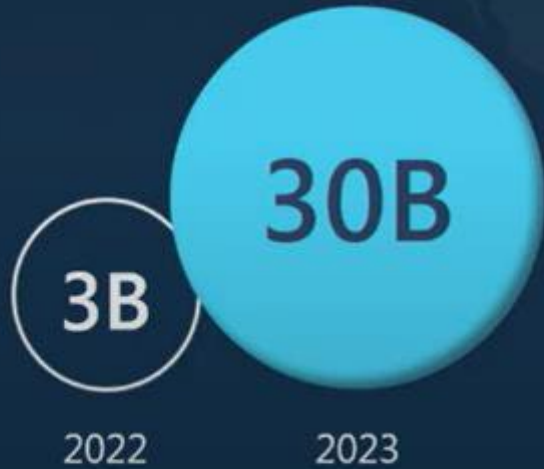
Who are the Threat Actors and what is the motivation?

- Ransomware extortion groups
 - Easy payday for extortion payments impacting operations
- Cybercriminal groups
 - \$60-\$250 average for a complete medical record
- Nation-state
 - Supply chain disruption, strategic destabilization
- Insider threats
 - Disgruntled or compromised internal users

We live in the most complex threat landscape in history

Speed, scale, and sophistication of attacks

Password attacks per month



Source: Microsoft

Rapidly growing cyber economy

Annual GDP



Source: Statista

Growing regulatory environment



250

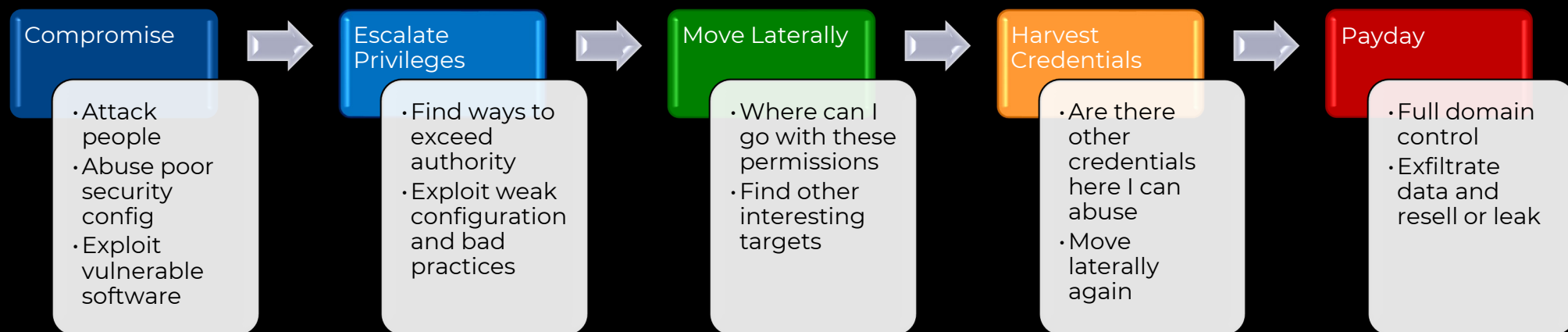
new regulatory updates tracked every day

Source: Microsoft

Top Risks for FQHCs

- Ransomware
- Fraudulent wire transfers
- Data breaches through vendors or direct
- Legacy / Outdated Systems
- Insider threats – accidental disclosure
- Under-resourced IT Teams

Anatomy of an attack

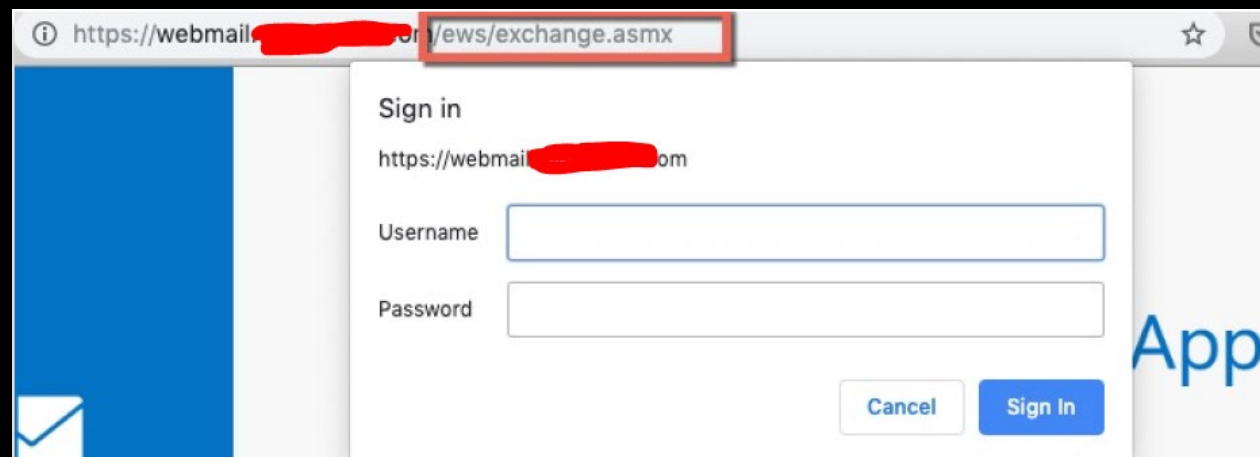


Let the games begin!

Reconnaissance on employees

Password spraying

46 min intervals to avoid lockout

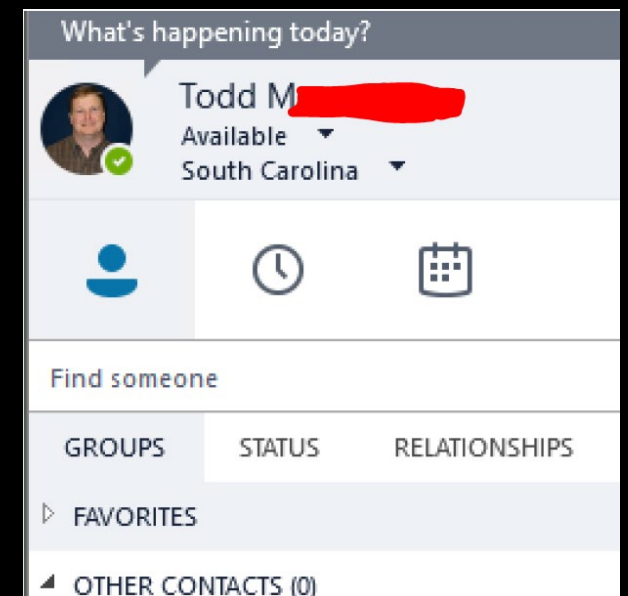
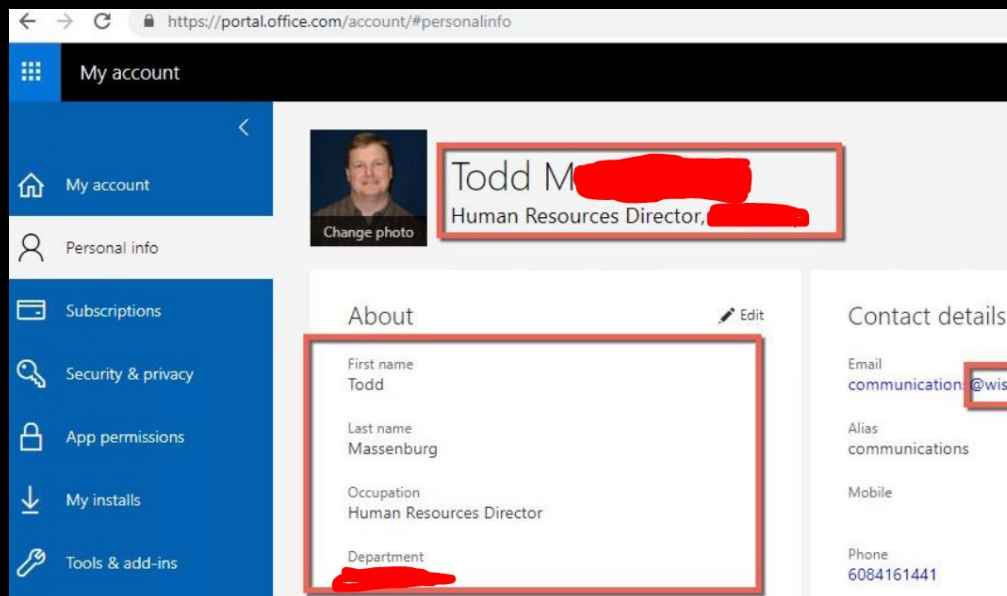


```
[ - ] 75.136.244.214:443 - Failed login: Laura.[redacted]:April2019!  
[ - ] 75.136.244.214:443 - Failed login: Godin.[redacted]:[redacted]2019  
[ - ] 75.136.244.214:443 - Failed login: Isiah.[redacted]:[redacted]19  
[ - ] 75.136.244.214:443 - Failed login: Scott.[redacted]:[redacted]19!  
[ - ] 75.136.244.214:443 - Failed login: Jon.[redacted]:Winter2019
```

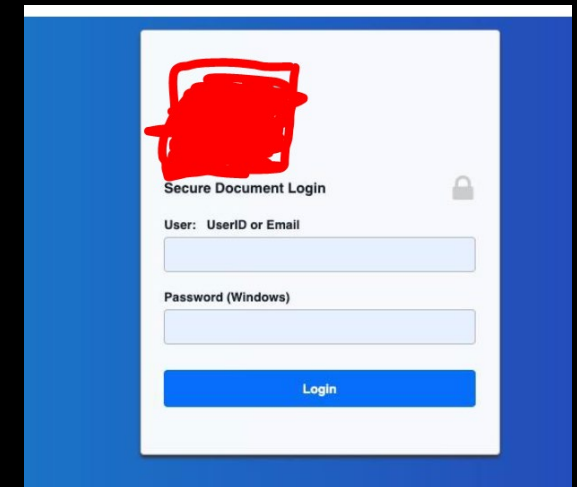
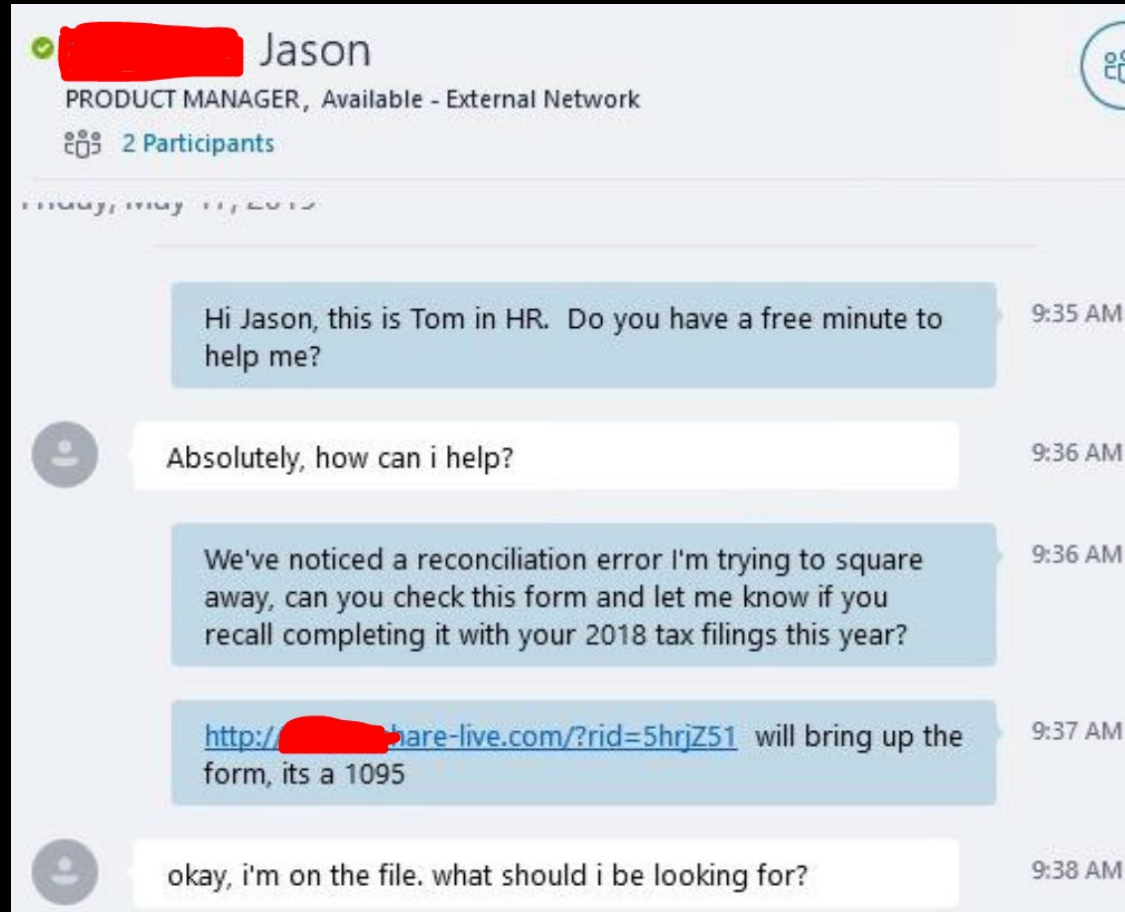
If at first you don't succeed...



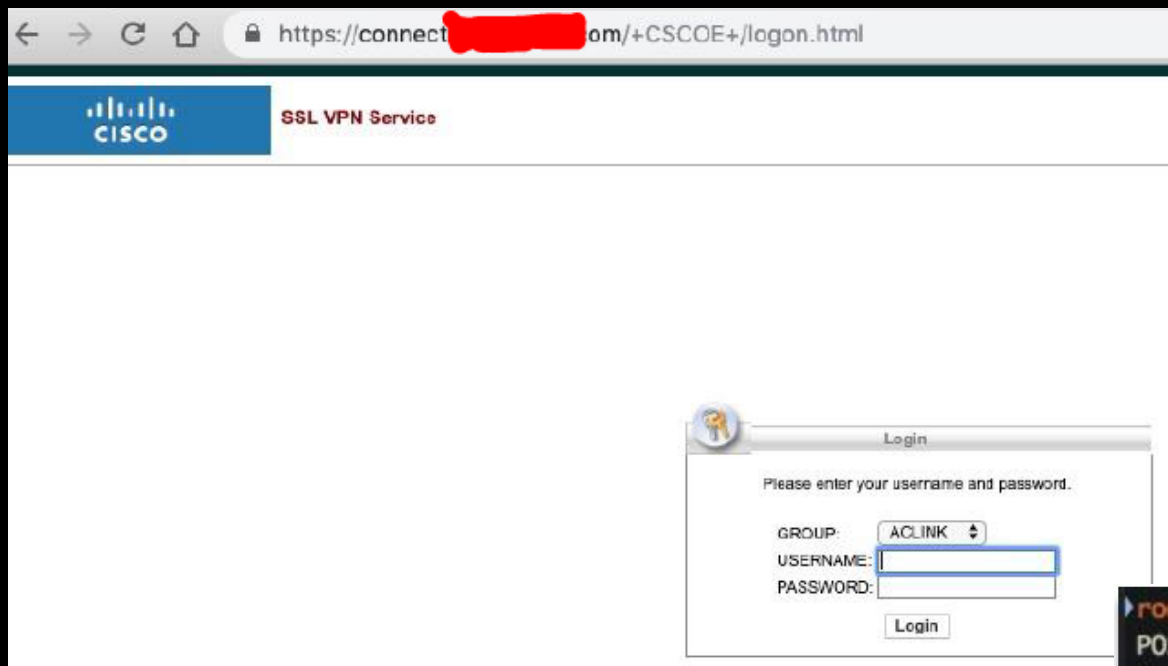
Use social engineering



Dupe employees to provide login credentials



We're in!



```
root@kalivm:linkedin# openconnect connect.[redacted].com
POST https://connect.[redacted].com/
Connected to 68.115.235.85:443
SSL negotiation with connect.[redacted].com
Connected to HTTPS on connect.[redacted].com
XML POST enabled
Please enter your username and password.
GROUP: [ACLINK|ACLINK_2]:ACLINK_2
POST https://connect.[redacted].com/
XML POST enabled
Please enter your username and password.
Username:travis [redacted]@[redacted].com
Password:
POST https://connect.[redacted].com/
Got CONNECT response: HTTP/1.1 200 OK
CSTP connected. DPD 30, Keepalive 20
Connected as 192 [redacted], using SSL
Established DTLS connection (using GnuTLS). Ciphersuite (DTLS0.

```

Domain Administrator credentials

```
root@kalivm:internal# cat enum.log | grep -Ei 'SrvAcct|marlyb'
index: 0x5da6 RID: 0x362a acb: 0x00000210 Account: marlyb      Name: Marly, Bob      Desc: (null)
index: 0x3d08 RID: 0xdbf acb: 0x00002210 Account: SrvAcct   Name: Service Account Desc: Service Account
user:[SrvAcct] rid:[0xdbf]
user:[marlyb] rid:[0x362a]
Group 'Backup Operators' (RID: 551) has member: ██████████\SrvAcct
Group 'Exchange Domain Servers' (RID: 1673) has member: ██████████\SrvAcct
Group 'Domain Admins' (RID: 512) has member: ██████████\SrvAcct
Group 'Domain Admins' (RID: 512) has member: ██████████\marlyb
Group 'Domain Admins' (RID: 512) has member: ██████████\marlyb
```

GAME
OVER

What could have prevented this?

Baseline Controls

- Multi-factor authentication for all external access and privileged accounts
- Employee awareness training and phishing
- Web/email filtering
- Real-time detection and response
- Tested data backup and recovery plans
- Regular vulnerability and penetration testing
- Web / DNS filtering
- Cybersecurity insurance

Level 2 controls

- Written information security program (WISP)
- Least privilege access
- Incident response
- Vendor Management
- Data encryption in transit and at rest
- Mobile device management

Innovative controls

- Zero Trust Architecture with continuous verification
- AI/ML powered threat detection and behavioral analytics
- Data classification, governance, and loss prevention
- End-to-end encryption with strong cryptography
- Ransomware attack simulations
- Purple team exercises

How does AI impact the threat landscape?



AI threats

Automated attacks

AI-powered social engineering

Data poisoning

Bias and discrimination

Exploitation of insecure credentials or excessive sharing

Supply chain data and privacy

Questions that leadership and Board should ask?

What are our top cybersecurity risks and how are we managing them?

How does our cybersecurity strategy support patient safety, data privacy, and operational continuity?

Who is accountable for cybersecurity across clinical, IT, and executive leadership?

Are we compliant with HIPAA, HITECH, and other applicable healthcare regulations?

How do we assess and manage risks from third-party vendors, especially those handling PHI?

If we experienced a ransomware incident, how long would it take to resume operations? How would we ensure continuity of care?

How do we promote cybersecurity awareness among clinicians, staff, and contractors?

How frequently do we review cybersecurity risks and incident reports at the board level?



Thank you!

Jeff Olejnik

Partner

jolejnik@wipfli.com

952.230.6488

wipfli.com

“Wipfli” is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.