

# Indian Health Service

## Building a Culture of Cybersecurity at IHS

---

ED CONLEY

DIS PSA TEAM

8/14/2024



# Creating a culture of cybersecurity

---

What is workplace culture?

How do you build workplace culture?

How do you build a workplace culture of cybersecurity?

What resources are available to help build a workplace culture of cybersecurity?



# What is workplace culture?

---

Defining “workplace culture.”

The IHS mission.

Benefits of workplace culture.



# How do you build workplace culture?

---

Leadership level, Team level, Individual level.

Creating workplace culture in a remote setting.

Recognizing fulfilment of workplace culture ideals.



# How do you build a workplace culture of cybersecurity?

---

Mature vs. immature workplace cultures or cybersecurity.

A culture of cybersecurity at the leadership level.

A culture of cybersecurity at the team level.

A culture of cybersecurity at the individual level.



# What resources are available to help build a workplace culture of cybersecurity?

---

DIS Website.

(<https://www.ihs.gov/oit/security/>)

CyberSecurity Awareness Month (CSAM).

(<https://www.ihs.gov/oit/security/ncsam/>)

Division on Information Security monthly newsletter.

(<https://www.ihs.gov/oit/security/resources/documents/infographics/dis-newsletters/>)

Policy and Security Awareness resource links.

(<https://www.IHS.gov/OIT/Security/Resources/>)



# Questions?

---

Ed Conley

IT Specialist (PSA)

Division of Information Security

Office of Information Technology

Indian Health Service

[Edward.Conley@ihs.gov](mailto:Edward.Conley@ihs.gov)







# Indian Health Service

## Building a culture of cybersecurity in IHS clinics and hospitals

REESE WEBER, MBA, CISSP

2024 IHS PARTNERSHIP CONFERENCE

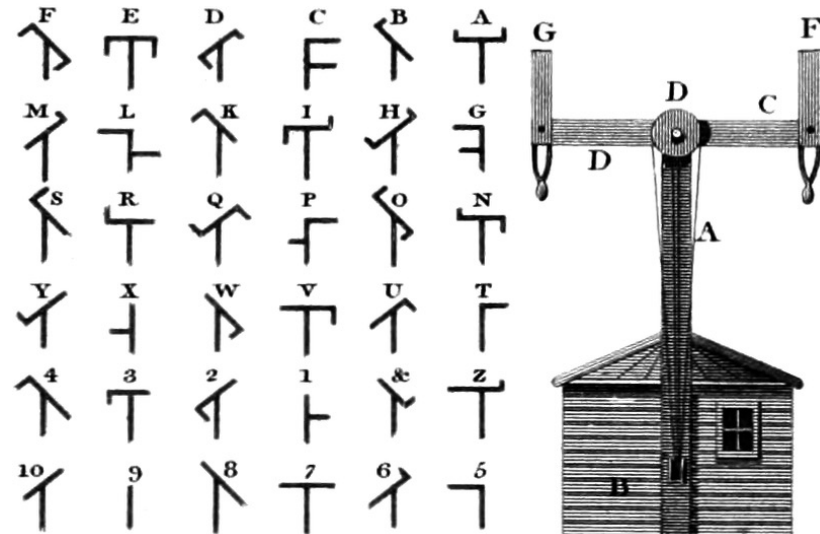


# When was the first Network hack?

---



1853 Optical Telegraph Network Hack  
Bordeaux, France



# Bath and Body Works Scam Website: Testimony of a sucker.



# Should I be embarrassed or am I just a human?

---

Being embarrassed means  
that you're human, and we  
**like you better for it.**

Nick Morgan

 quote fancy

# Human Beings – the most easily exploitable aspect of cybersecurity

---



A Threat Vector is the method that attackers use to get into your network.

Humans are the NUMBER ONE threat vector that attackers use to launch cyberattacks.

All of the most sophisticated technologies and tools on the market won't prevent your employees from giving up their credentials to the bad guys. User Awareness is the ONLY way to combat this exploitable vulnerability.

Social engineering is based on psychology, not technology.

90% of cybersecurity breaches start with a phishing email

# Adopt a human net posture!

---



If you get a suspicious email, it should always be reported to your respective incident response team.

But...why stop there? Let a coworker know – “Hey I got a weird email, be on the lookout.”

Did several people get the same or similar messages? Maybe you could send out a message warning your colleagues.

Do you use collaboration software? Send a message through Microsoft Teams, or whichever you use!



# Anatomy of a Phishing Victim

## Empathetic

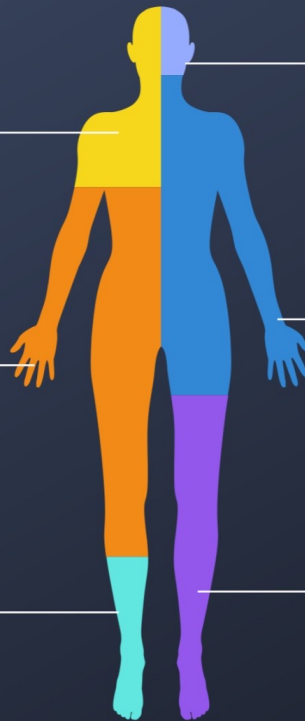
Bonding easily with others creates higher susceptibility to emotionally-motivated romance and confidence scams.

## Distractable

Victims who skim emails and miss suspicious errors, or those enticed by something new/exciting, are more easily scammed.

## Trusting

The scammed tend to take what they read at face value, exercising less suspicion overall.



## Impulsive

Quickly acting, especially when coupled with a sense of urgency, increases a victim's likelihood of making thoughtless errors, such as clicking on malicious links or accepting unidentified connection requests.

## Obedient

Followers are more likely to do what they're told (click a link, send money, provide private information) regardless of who's doing the directing.

## Uninformed

These folks may have disdain for data privacy or simply lack tech literacy. The less known about phishing scams and IT security protocols, the better for scammers.



# Phishing Exercises

---

Acknowledge successes!

Acknowledge “failures”, which should be considered “opportunities for learning”

Be effusive with your praise, and transparent about the results.

Talk to your director or CEO about possible incentives for 0% click rates or other desired outcomes.

Don't tell anyone when the exercise launches!





# Don't punish accidental cybersecurity violations

---

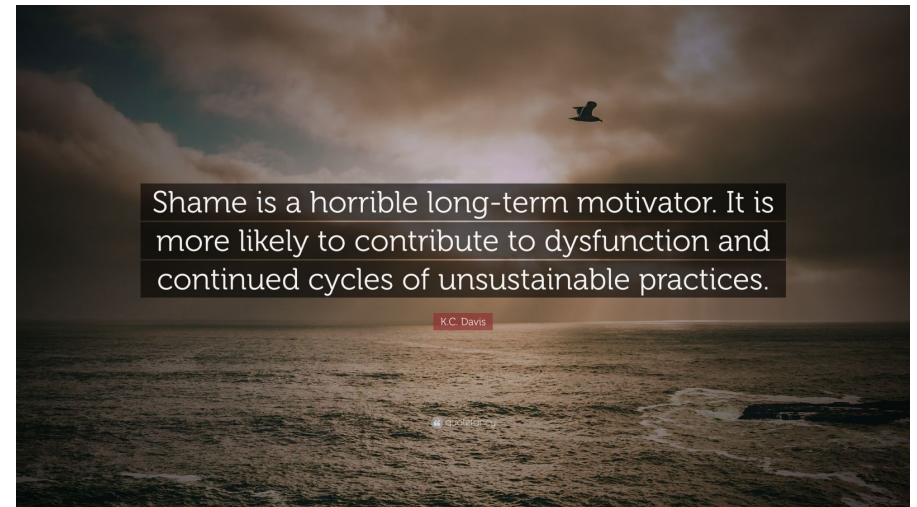
Shame doesn't motivate or teach employees.

We are all vulnerable to exploit, and mistakes happen.

We want employees to let someone know if something happened! Fear of retribution may prevent someone from speaking out.

Encourage your employees to be forthright about their mistakes, and use them as (maybe anonymous?) examples of an employee making a mistake and coming forward, and commend them for it!

Commend your employees for reporting ANY suspicious activity!



# Do folks know who to reach out to, and how?

---

- Who is your information security contact at your facility?
  - The HIPAA Security Rule requires every medical organization to have an identified security contact.
  - If you don't have someone assigned, you simply need to delegate a POC, create a 1 page policy that documents the person and their contact information.
  - They do not have to be technical per se, they would only need to know how to escalate incidents and be a central point of contact for disseminating pertinent advisories for their facility.
- Who is your area information system security officer (ISSO)?

You can check the IHS website - <https://www.ihs.gov/itservicedesk/areait/> - to see who your respective ISSO is.



Alaska Area  
ISSO: Vacant

Albuquerque Area  
ISSO: Bernie Jojola  
ISSO Phone: 505-256-6701

Bemidji Area  
ISSO: Anthony Lafontain  
ISSO Phone: 218-444-0459

Billings Area  
ISSO: Clint Muschamp  
ISSO Phone: 406-247-7167

California Area  
ISSO: Reese Weber  
ISSO Phone: 916-930-3981 x307

Division of Engineering Services (DES)  
ISSO: Mary Moore  
ISSO Phone: 202-834-2796

Great Plains Area  
ISSO: Brad Flom  
ISSO Phone: 605-335-2509

IHS Headquarters Office  
ISSO: Zhi Cheng  
ISSO Phone: 240-535-2930

Nashville Area  
ISSO: Scott McCoy  
ISSO Phone: 615-467-1525

Navajo Area  
ISSO: Vanessa Segay  
ISSO Phone: 928-871-1303

Oklahoma Area  
ISSO: Amy Rubin (Acting)  
ISSO Phone: 405-951-3732

Phoenix Area  
ISSO: Lewis "Rocky" Lackman  
ISSO Phone: 602-364-5278

Portland Area  
ISSO: Douglas J. Bristow  
ISSO Phone: 503-414-7753

Tucson Area  
ISSO: Bernard Howell  
ISSO Phone: 520-295-2502

## The IHS Area Information Systems Security Officers



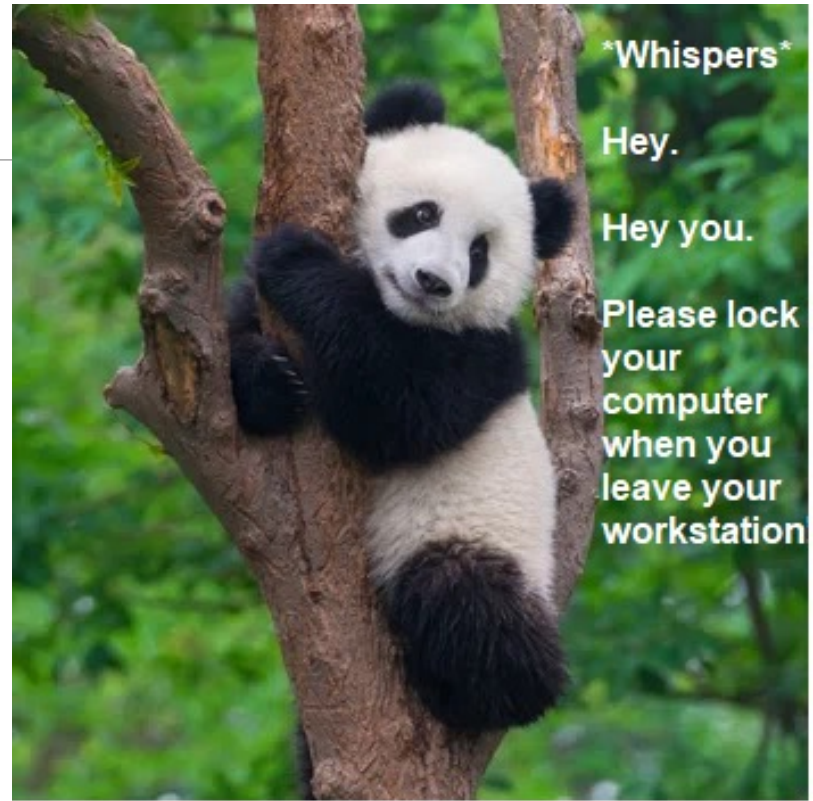
# Making Cybersecurity Fun

---

Ways to incorporate cybersecurity in fun ways to further promote the cybersecurity culture

- Find ways to incentivize reporting of privacy and security violations or suspicions.
  - You could randomly draw a name from employees who reported events monthly to win a prize. Report a phishing email, and win the privilege of wearing jeans! Or 59 minutes of admin leave? It can be anything, as long as it gets people involved and engaged.
- Empower your employees to motivate each other! Hold a contest of “Who can create the best/funniest/most clever cybersecurity slogan?” Or “who has the best/most interesting experiences with cybersecurity”. You can highlight the winners in a staff meeting, an email blast, etc.
- Have a sign making contest, where people make funny or brilliant signs warning folks about vulnerabilities.
- Outsource ideas! Ask employees to submit their suggestions on how to expand cybersecurity awareness. Make sure the employees are recognized for their contributions.



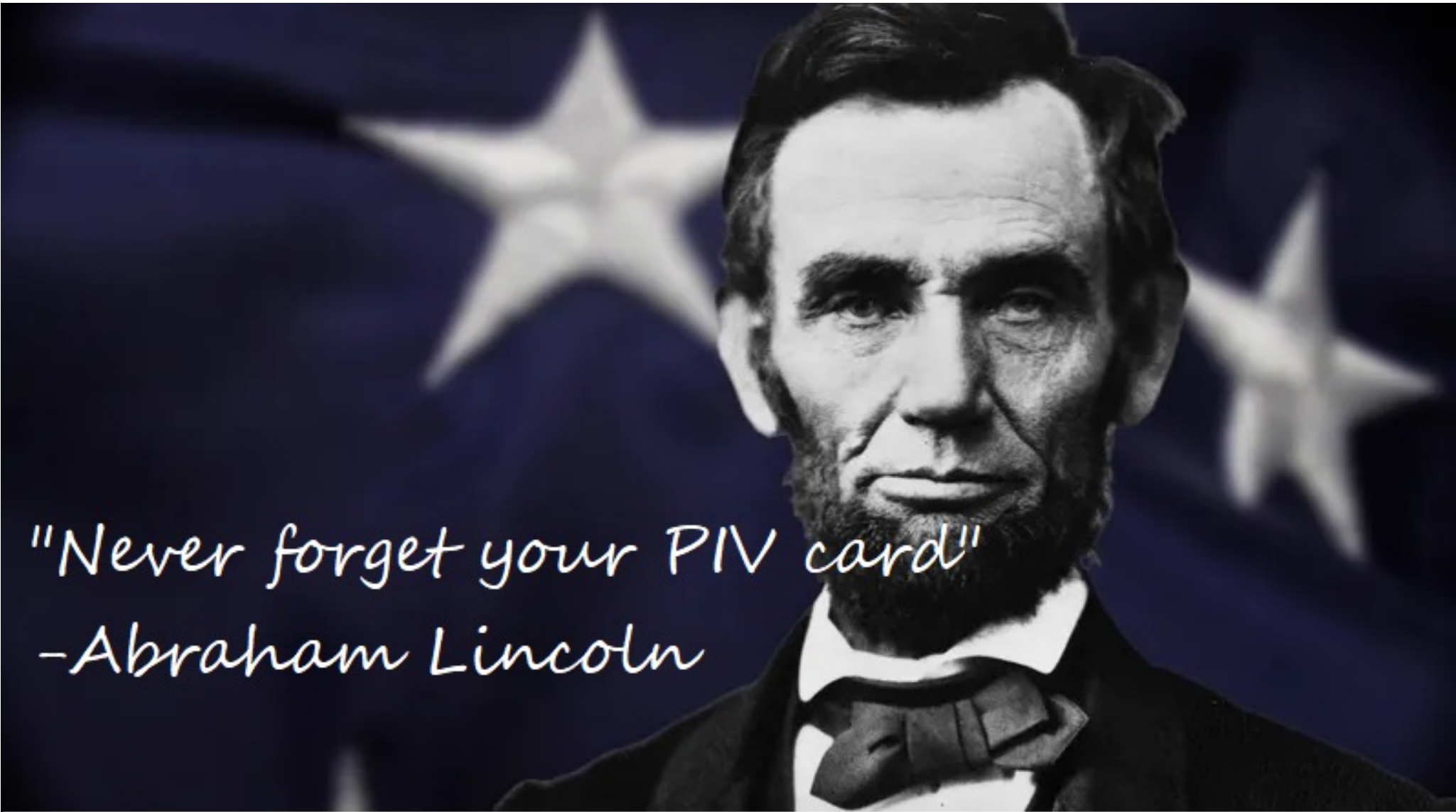


**I trusted you with my credentials!**



**You should NEVER share your credentials with anyone**





*"Never forget your PIV card!"*

*-Abraham Lincoln*

# Upcoming TribalHub Cybersecurity Events

---





# Questions?

---

Reese Weber, MBA, CISSP

Chief Information Security Officer and Privacy Coordinator

Indian Health Service, California Area

916-930-3981 x 307

[Theresa.weber@ihs.gov](mailto:Theresa.weber@ihs.gov)

<https://www.linkedin.com/in/reese-weber-mba-cissp-6085203b>



# References:

---

Anatomy of a phishing victim <https://baisecurity.net/blogs/anatomy-of-a-phishing-victim/>

Free cybersecurity posters <https://caniphish.com/free-cyber-security-awareness-posters>

CISA <https://www.cisa.gov/>



