CREATING A SECURITY FOCUSED CORPORATE CULTURE

AKA: THE POLITICS OF SECURITY

WHAT IS THE PROBLEM?

- Almost 58% of organizations that had security incidents over 2017 blamed them on insiders
- 45% of respondents, whether or not they experienced a security incident, still see their own employees as the biggest threat to security
- The majority of respondents have only partial visibility into what is happening in the cloud, and only 28% of organizations have visibility into IT staff activity

Taken from the Netwrix 2018 Cloud Security Report

WHAT IS THE PROBLEM?

- Phishing is the number one attack vector
- People will circumvent security when inconvenient
- People are the one thing that will never change
- Disconnect between security and the rest of the business

WHAT SECURITY TYPICALLY DOES

- Focus on technology
- Ineffective Training
- Forget the “human element”
- Take themselves too seriously

FOCUS ON TECHNOLOGY

- IDS
- Firewall
- Email tools
- DLP
- Two factor authentication
- Anti-malware tools

INEFFECTIVE TRAINING

- Training non-technical users on very technical topics
- Unnecessary information
- Long-winded
- Communicate too often

FORGET THE "HUMAN ELEMENT"

- Think of users as insider threats or liabilities
- Negative reinforcement
- Lack of understanding of what matters to end user

TAKE THEMSELVES TOO SERIOUSLY

- Humor is discouraged
- Mistakes are not admitted
- Communication is dry

WHAT SECURITY SHOULD DO

- Stop using words like threat, liability, problem, idiot, etc.
- Start at the top – involve the highest-ranking person possible
- Focus on what makes security awareness meaningful to the end user
- Let them know that it's ok to make mistakes
  (***inform Security as soon as it happens!***)
- Most important: CHANGE YOUR ATTITUDE

WHAT SECURITY SHOULD DO

- Bring an element of fun to security awareness
  - Games
  - Training videos
  - Mock phishing attacks
  - Incentives
- Positive reinforcement
- Keep it brief