Shifting the Human Factors Paradigm in Cybersecurity

Calvin Nobles, Ph.D.

March 15, 2018

AGENDA

- Human Factors
- Cybersecurity – The Ugly Reality

A Famous Quotes

"Companies spend millions of dollars on firewalls, encryption and secure

access devices, and it's money wasted, because none of these measures address the weakest link in the security chain." [people]

– Kevin Mitnick

Convicted in the USA for hacking major corporations, and now a world recognized security advisor.

"If you think technology [alone] can solve your security problems, then you don't understand the problems and you don't understand the technology."

– *Bruce Schneier*

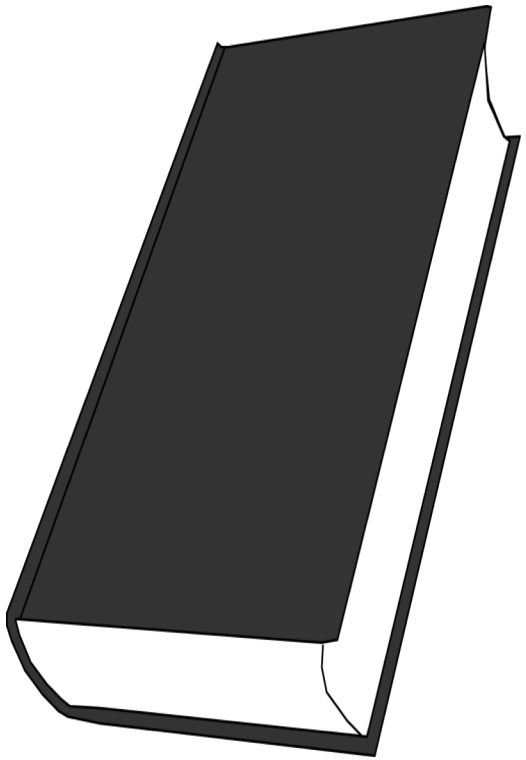
"Only amateurs attack machines; professionals target people"

– Bruce Schneier, 2000

Humans are the Foundation of Cybersecurity

Our Story

- **$90 Billion** global cost of information security (2017)
  - Forecasting $113 Billion in 2020
- **90%** of cyber incidents are human-enabled
- **Complex cybersecurity operations**
  - **Security fatigue / high tempo**
- **Underinvestment** in cybersecurity training
  - Technology remains the priority
- Increase in targeting people
  - Tactical objective – people
  - Strategic objective – sensitive data, intellectual property, and financial and informational assets



Human Factors

The study of human behavior on physical and cognitive performance in information security.

"Achilles Heel" of the cybersecurity

Complex Cyber Ecosystems

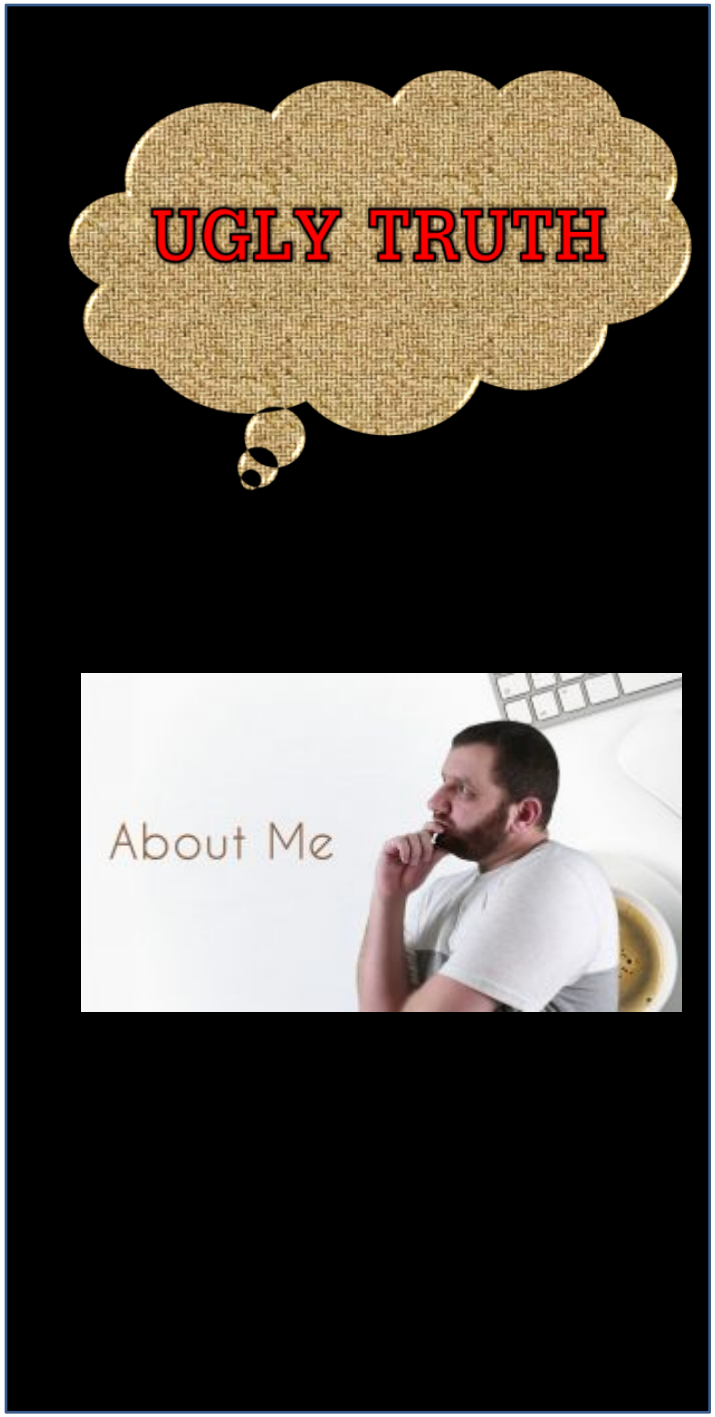
- ❑ Over confident in technology, compliance
- ❑ Regulations, security controls, compliance
- ❑ Lacks focus from stakeholders

Sophisticated attacks aimed at people

- **In 1996, DoD invested $220 Million in Human Factors**

Human Factors

- Witnessed violations of cybersecurity policies
- Open all emails at work
- Logged in using unsecure public networks
- Used approved devices for work at home
- Downloaded unapproved software at work
- Shared passwords with co-workers
- Of organizations lack a cyber strategy
- Increase angler phishing in 2016



Human Factors

Data Breaches	ID Attitudes	Automation	Organizational Culture	Performance
52% of data breaches cost ($4Million per incident)	Need to mitigate dangerous attitudes	Information Overload	Address human factors Make a Priority	Impact performance, Production, Profits

Leading Industries in Human Factors

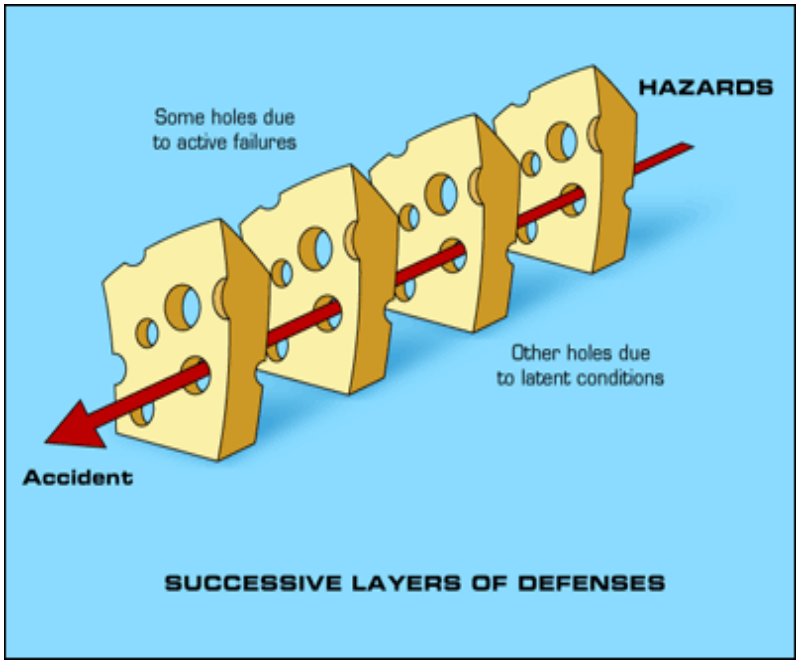
Aviation

Safety

Nuclear Power

Medicine

Space Exploration



Human factors success driven through organizational cultural

COMMON MISTAKES

Made by Cyber Professionals

- Misconfigured Network Settings
- Password Management (poor)
- Technology vulnerabilities
- Privilege Creep
- Violation of Standard Operations Procedures
- Cognitive Distractions
- Non-compliant Behavior
- Leadership Directed Actions

Human Factors, Technology, Automation Impacts

Human Factors Impacts	Too much Technology Impacts	Automation Impacts
Core Pillars easily Disrupted	Degradation of Performance	Changes in the decision-making process
Lack of Human Factor Objectives	Demanding Environment	People become information managers
Too much Technology	Constant Change	Require in-depth technical knowledge of systems
Inundated with Information	Cognitively challenging	Creates complacency degrades proficiency
Misaligned Business and Security Objectives	Anxiety /stress fatigue	Information overload
	Information overload / automation misuse	Software coding errors
		Delivery time supersedes cyber defense

Culture and Human Factors Principles

Integrity

Process Compliance

Expertise

Empowerment

A questioning attitude

Standardization

Human Performance Standard of Excellence

Cybersecurity Training

- Need specialty cybersecurity specific training
- Train to the operational shortfalls
  - DevOpS
  - Privileged creep
  - Data breaches
  - Misconfigurations
  - Ransomware attacks
  - Cyber-attacks
- Internal Training Programs
  - Apprenticeship Program

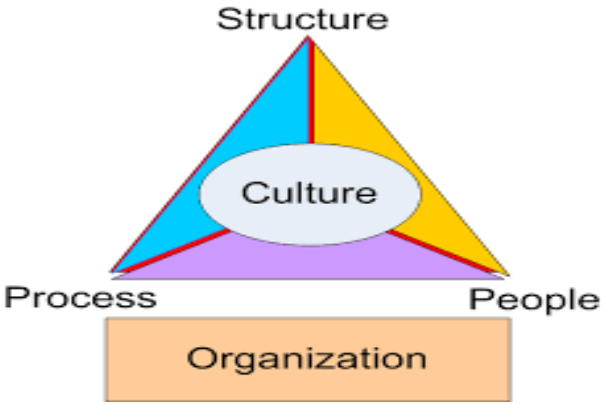
Human Factors

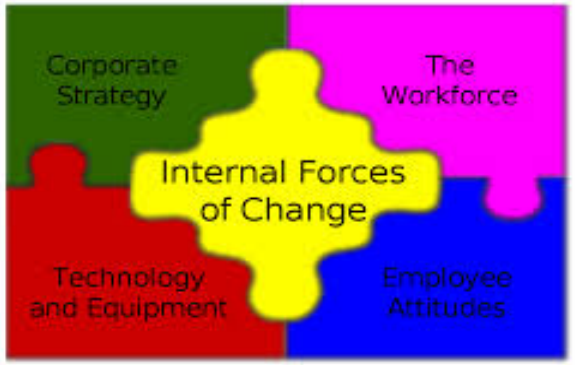
- C-Suite driven
- Increased security
  - Accuracy
  - Prioritization of effort
  - Identify critical phases/operations
  - Enhanced operability of systems

  - Increased profit and business proficiency

Bridging the Gap in Cybersecurity

The Cyber Human Error Assessment Tool

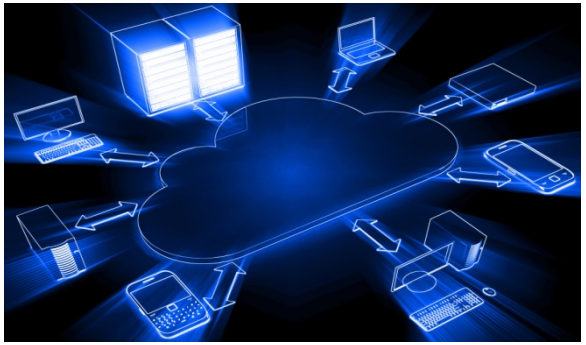




CHEAT	Focus Areas	Expertise	Culture	Organizational Practices
- Designed to support proactive assessments cyber-security vulnerability and to identify human-related root causes post-incident. - Eliminate or mitigate identifiable risks.	-People -Organization -Environment -Technology	-Cyber -Psychologists -Human Factors Experts -Technologists	-360 degree organizational cyber assessment for all employees -Integrate cultural objectives in the strategy -Investigative Team	-Impact -Performance -Production -Profits

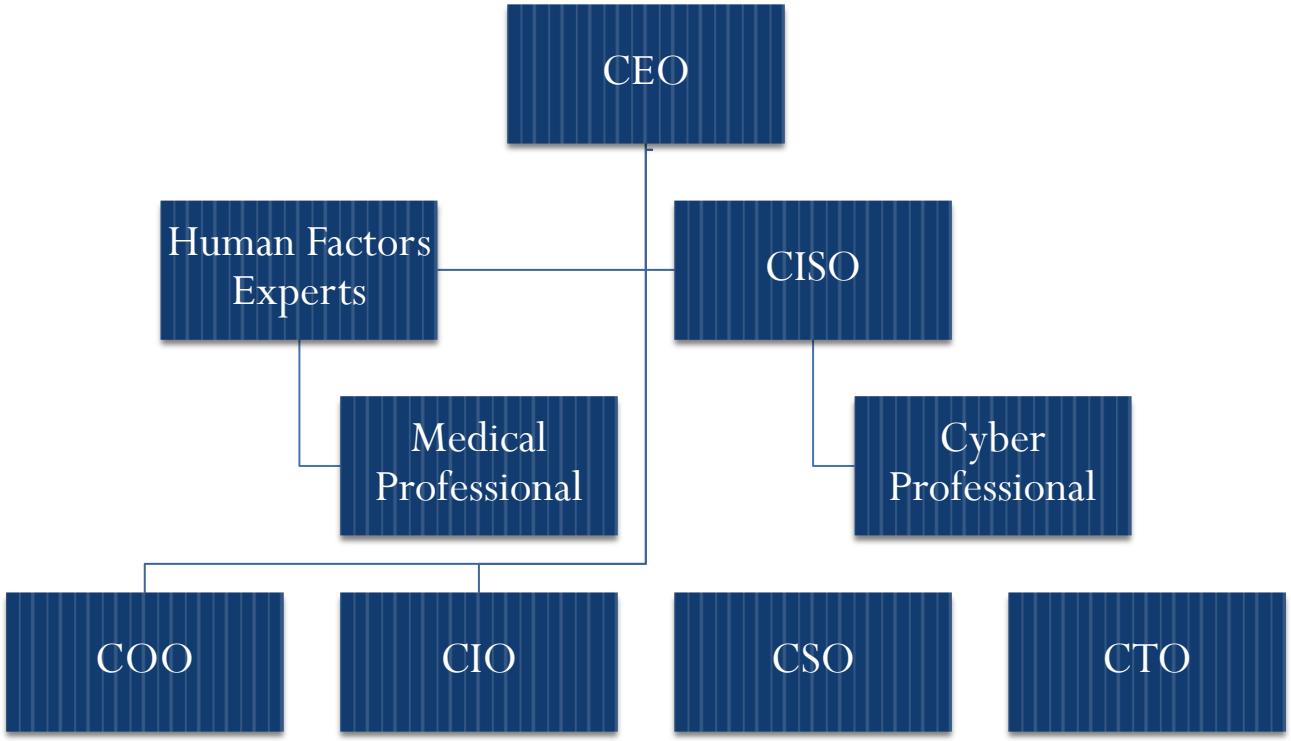
Need more theoretical foundations that lead to institutional practices in human factors

What is Your Human Factors Platform?



Establishing a Platform

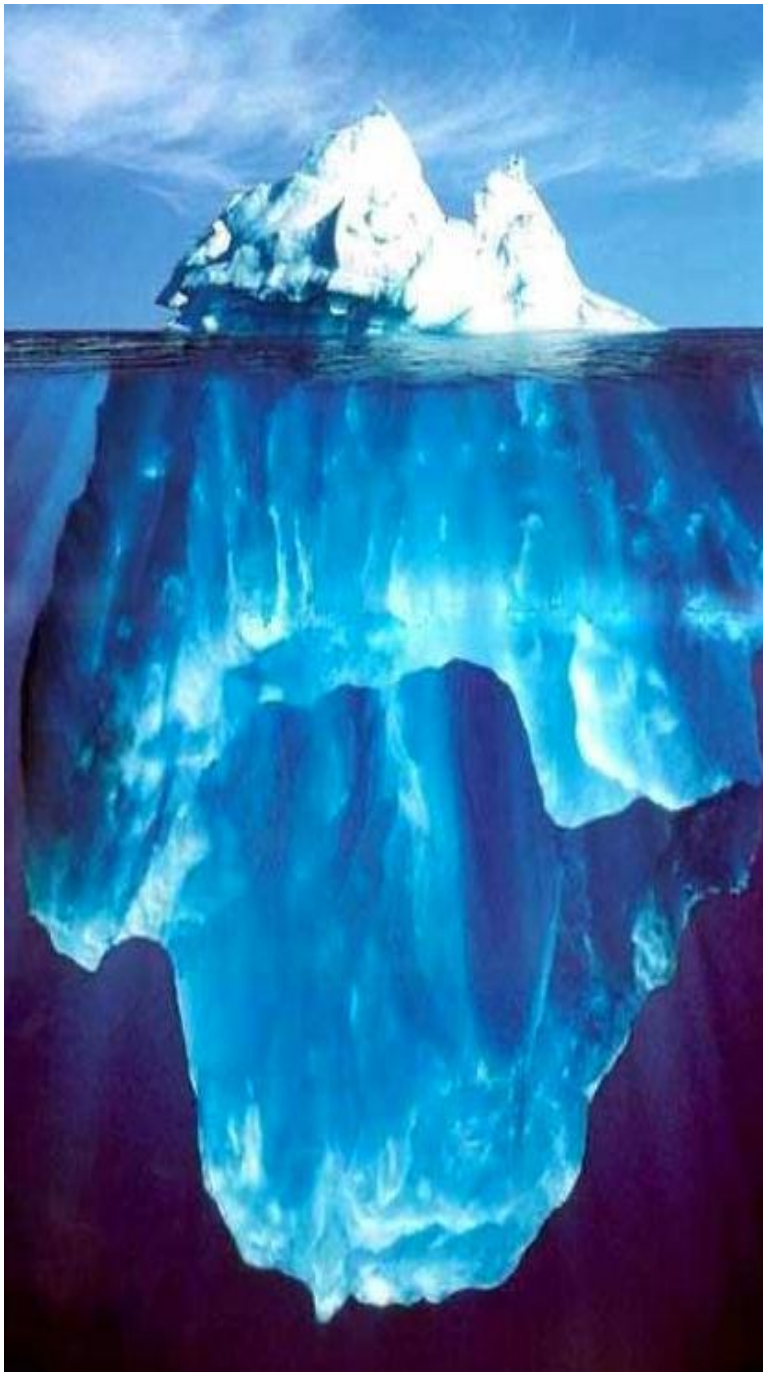
Executive Human Factors Council



(Generic Construct)

The purpose of this council is to drive enterprise-wide human factors initiatives.

The True Enormity



The true magnitude of the human factors problem