Human Factors and Energy Sector Cybersecurity

CSP001_C_E

PRESENTATION BY:
DR. RICARDO G. LUGO, TALTECH
DR. KITTY KIOSKLI, TRUSTILIO
PROF. PARESH RATHOD, LAUREA

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

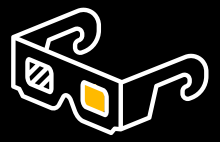
Project Agreement no. 101083594

Agenda

Learning outcomes
Psychological aspects of Cybersecurity in Energy sector
Psychosocial aspects
Future trends

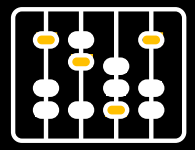
Goals: Who-What-Why you need to take this training

WHO



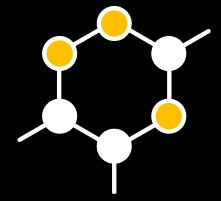
Open to all

WHAT



Foundation understanding of Human Factors for cybersecurity in energy sector

WHY



Equipping participants with the knowledge and skills necessary to understand how human aspects influence in energy sector cybersecurity

Benefits to Participants

- Level of Training Module: Basic
- Cybersecurity Professional Training
- Rooted with European Cybersecurity Skills Framework
- Cutting-edge insights from industry-academic experts
- Helps with skills development and career advancement

Training Topics

- Introduction to Human Aspects of Energy Sector Cybersecurity
- Psychological and Social Factors in Energy Sector Cybersecurity
- Human Vulnerabilities in Energy Sector Cybersecurity
- Organisational Culture, Communication, and Cybersecurity
- Communication and Collaboration Across Domains
- Decision Making at Strategic, Operational, and Tactical Levels
- Training, Awareness, and Communication Programs for Energy Sector Personnel
- Future Trends, Challenges, and the Role of

Learning Outcomes

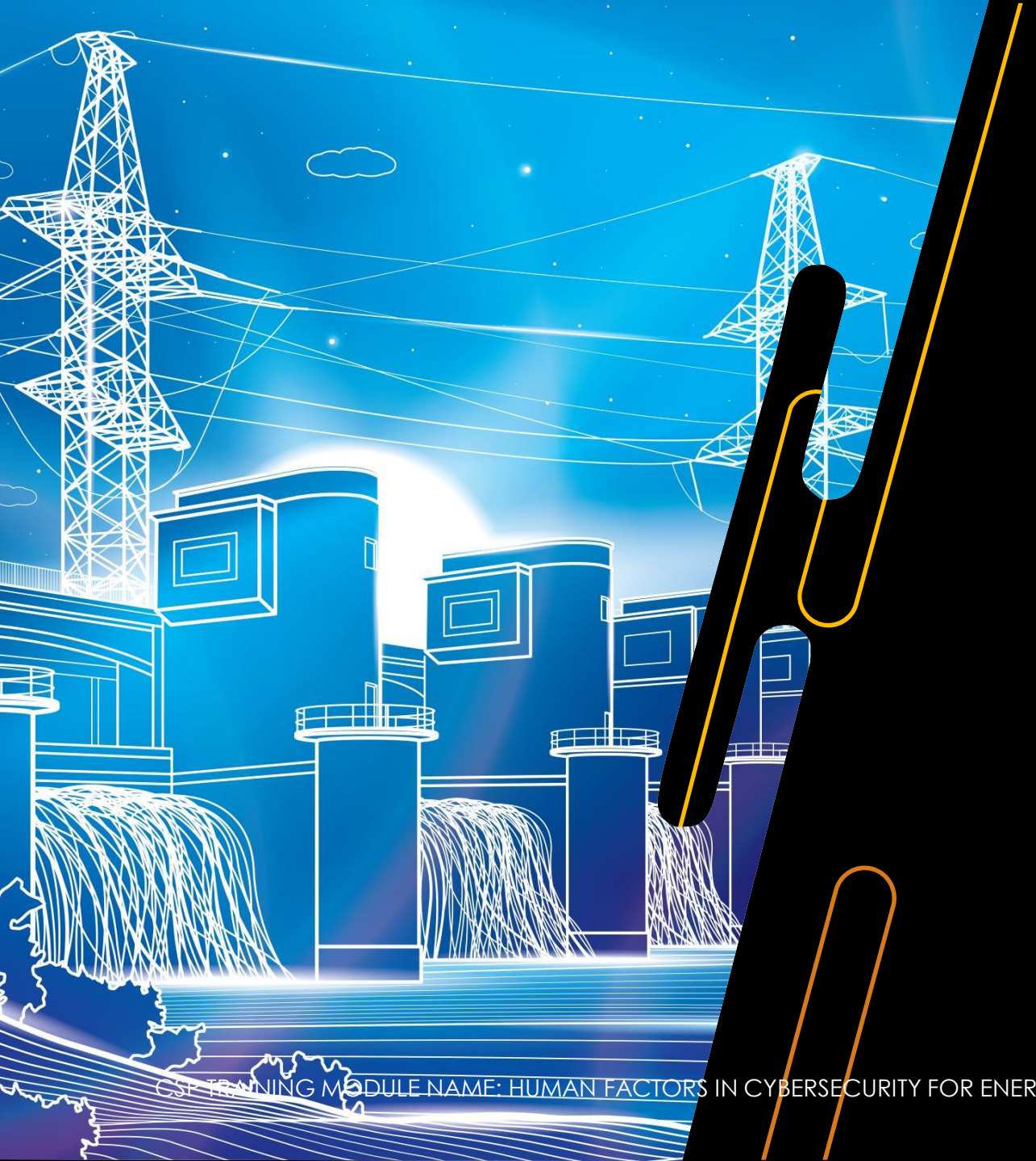
Knowldge

- Gain an understanding of the psychological, social, and organizational elements that shape cybersecurity actions within the Energy Sector.
- Understand the critical role of communication and teamwork in bolstering energy sector cybersecurity across different sectors.
- Recognize the profiles and strategies of adversaries targeting energy sector operations.

Learning Outcomes

Competencies

- Understand the discussions relevant to energy sector cybersecurity at various levels of decision-making.
- Be able to foster an environment of transparent communication and teamwork focused on energy cybersecurity.
- Reflect on cybersecurity decision-making with an awareness of how human factors play a role in the energy sector.
- Be able to identify human-centric threats and vulnerabilities in energy operations.



Importance of Human Factors:

Overview of Energy Sector Cybersecurity

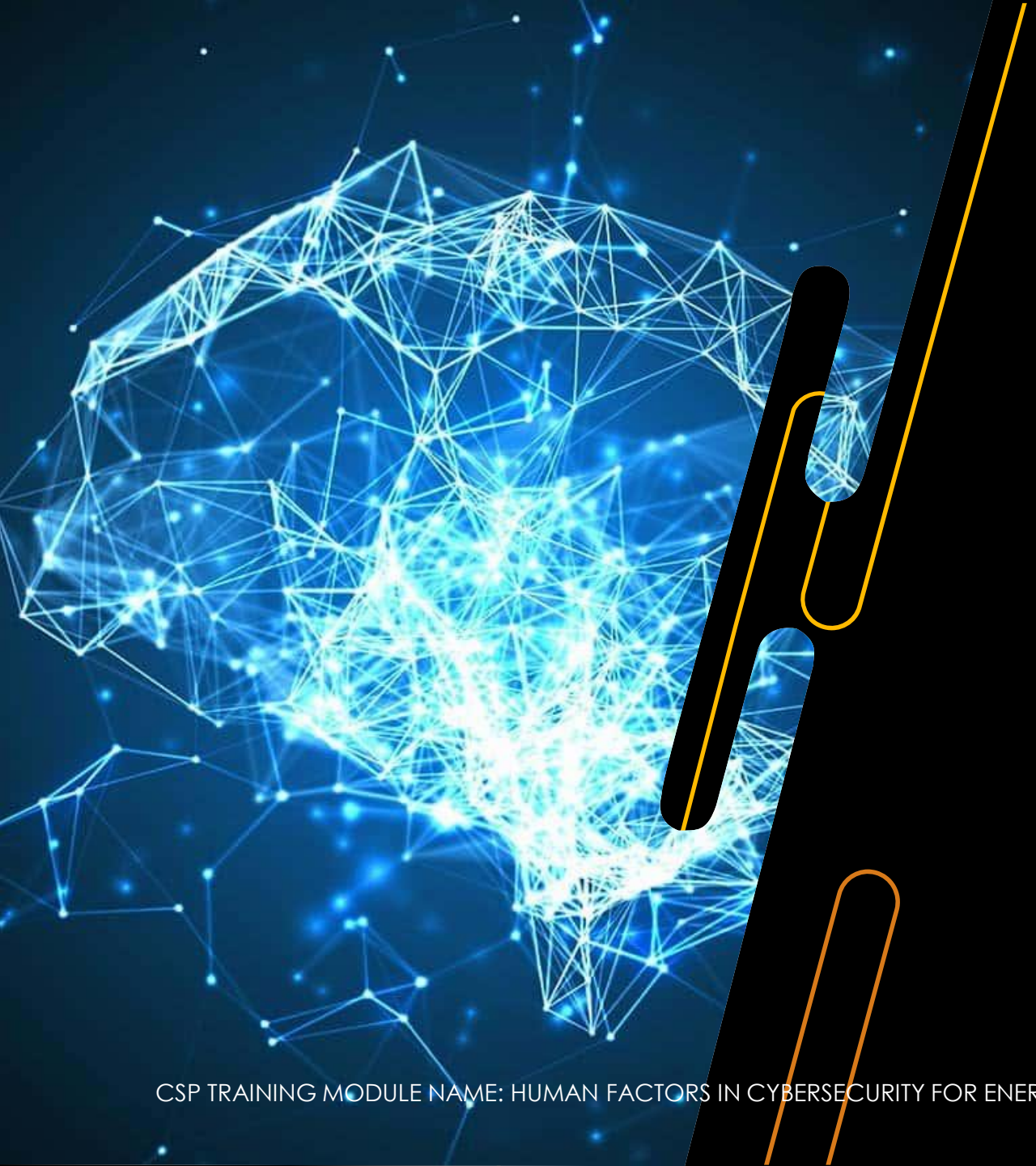
- Importance of cybersecurity in energy sector operations.
- Unique cybersecurity challenges in the energy sector.
- Role of human factors in energy sector cybersecurity.
- Identified Threats:
- IT/OT conversion
- Low priority and confidence
- 2023: 250+ 3rd party breaches
- Examples that will be used:
- Ukranian Power Grid Attack 2015
- Colonial Pipeline
- Stuxnet

- Raise your hand if you have:
  - Clicked on a link (from anyone)
  - Have a complex passphrase (?)
  - Use the same password on different sites/apps
  - Haven't changed your password in the last 30 days
  - Given your phone/pc to someone else to use
  - Have simple login to phone/pc
  - Not updated pc/phone in last 7 days

Importance of Human Factors:

Human Factors in Cybersecurity

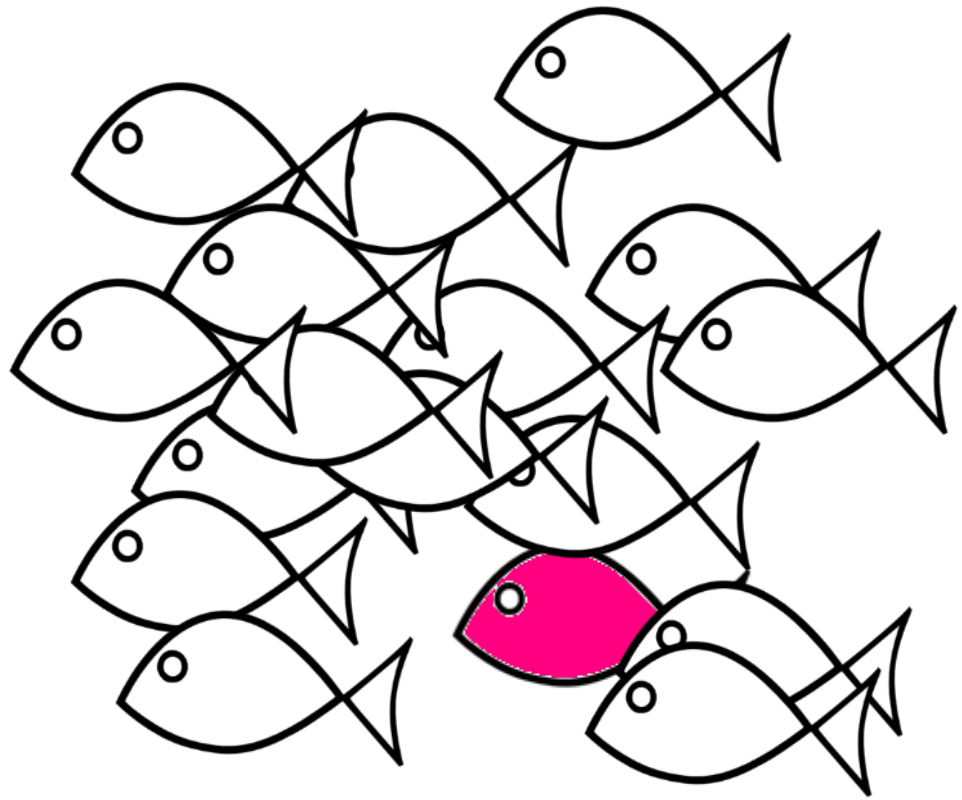
- Definition and significance of human factors in cybersecurity.
- Common human errors contributing to cybersecurity breaches.
- Strategies to mitigate human-related risks.



Importance of Human Factors:

Psychological Implications

- Psychological aspects influencing cybersecurity behaviours.
- The effect of cognitive biases on security decisions.
- Implementing psychological principles to enhance cybersecurity measures.

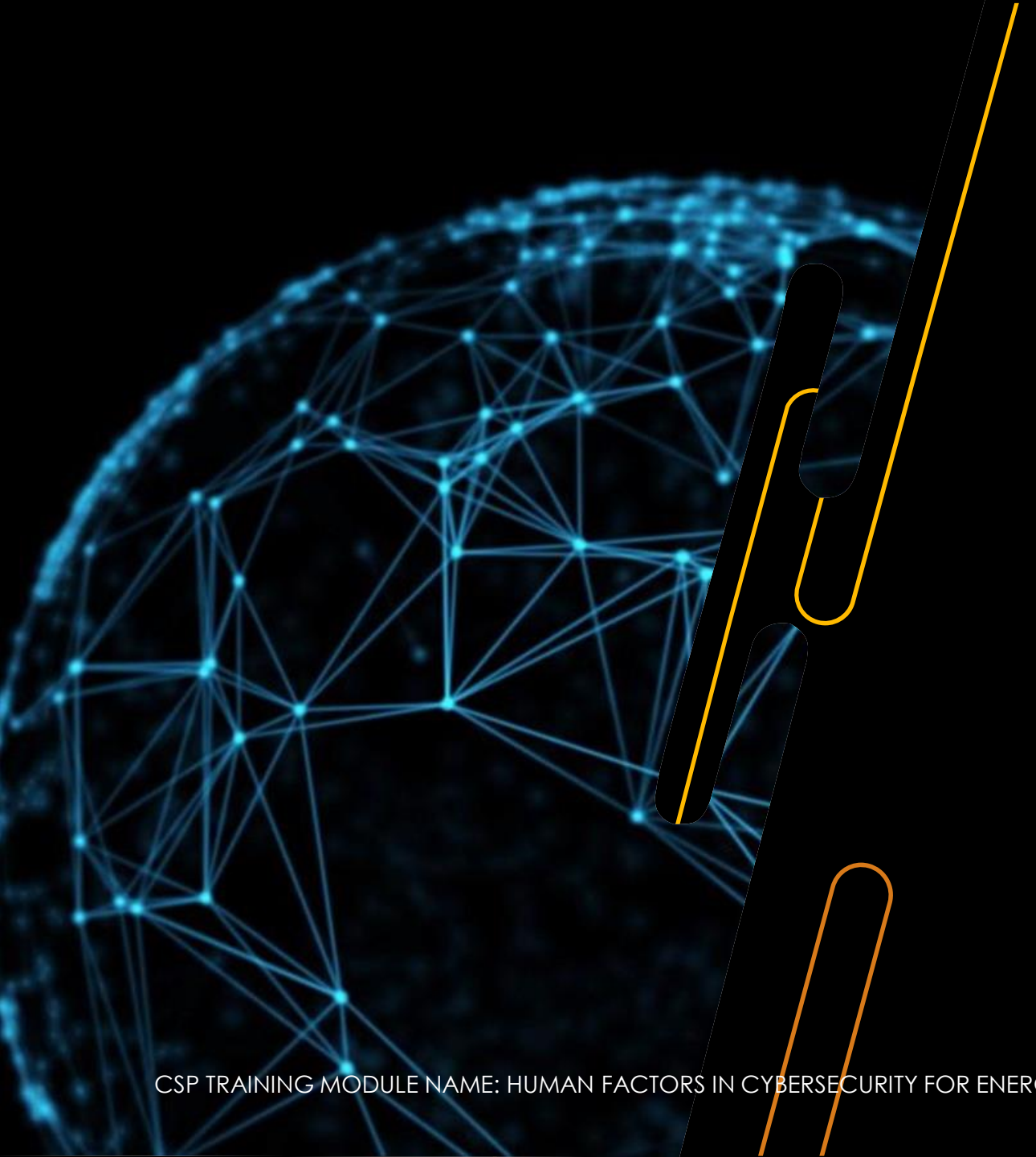


Cognitive Dissonance - Cognitive

P)?

"3.1.1 NameDrop Data [...] Any and all data generated and/or collected by NameDrop, by any means, may be shared with third parties. For example, NameDrop may be required to share data with government agencies, including the U.S. National Security Agency, and other security agencies in the United States and abroad. NameDrop may also choose to share data with third parties involved in the development of data products designed to assess eligibility. This could impact eligibility in the following areas: employment, financial service (bank loans, insurance, etc.), university entrance, international travel, the criminal justice system, etc. Under no circumstances will NameDrop be liable for any eventual decision made as a result of NameDrop data sharing."

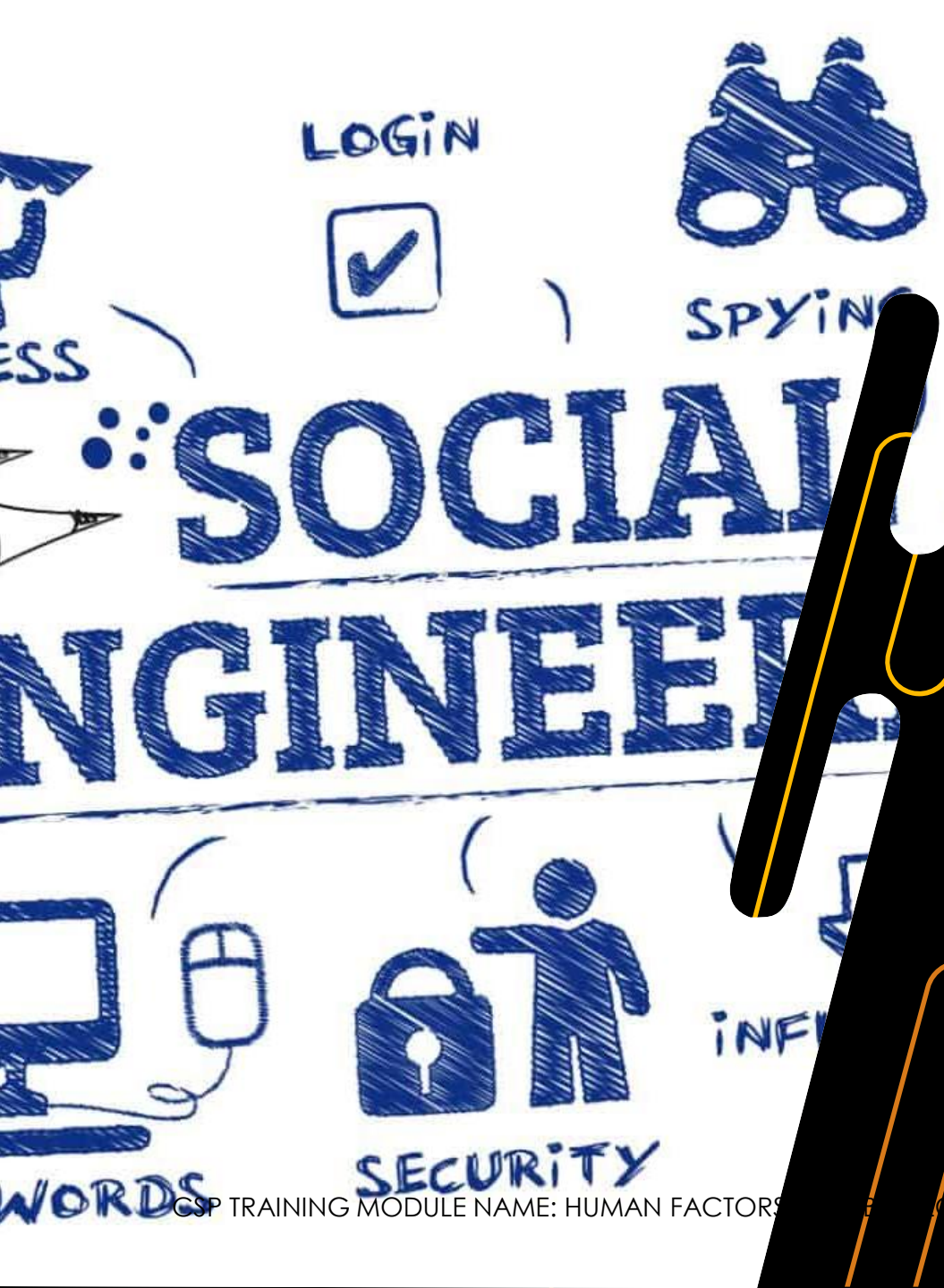
2.3.1 Payment types (child assignment clause): In additio to any monetary payment that the user may make to NameDrop, by agreeing to these Terms of Service, and in exchange for service, all users of this site agree to immediately assign their first-born child to NameDrop, Inc. If the user does not yet have children, this agreement will be enforceable until the year 2050. All individuals assigned to NameDrop automatically become the property of NameDrop, Inc. No exceptions.



Importance of Human Factors:

Social Influence

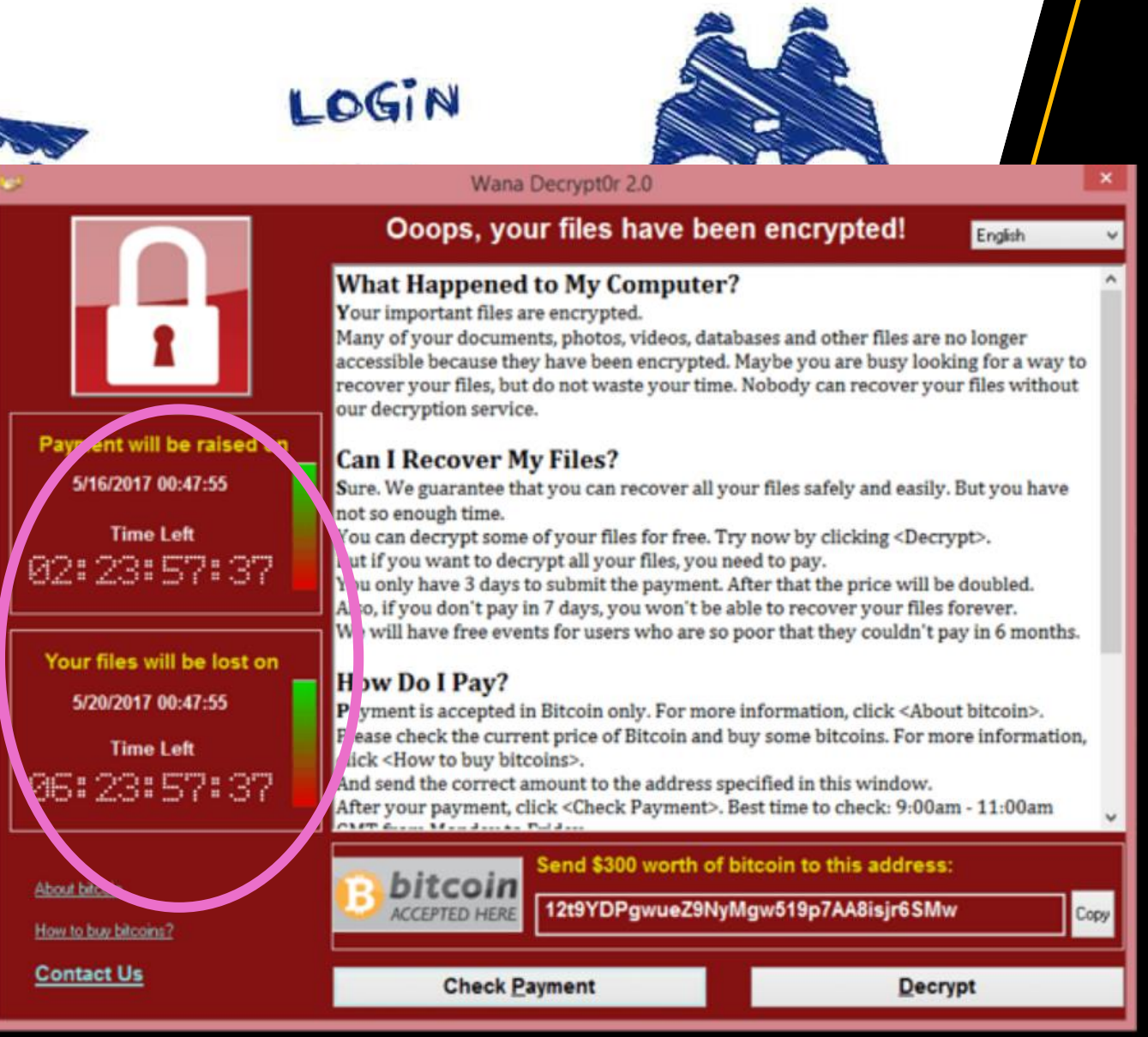
- Impact of social dynamics on cybersecurity practices.
- Role of organizational culture in shaping cybersecurity behaviours.
- Importance of social engineering awareness.



Importance of Human Factors:

Social Engineering

- Importance of social engineering awareness.
- Social Engineering
- Reciprocity; Commitment and Consistency, Social Proof; Authority; Liking; Scarcity



Importance of Human Factors:

Social Engineering

- Ransomware
- Scarcity and reciprocity

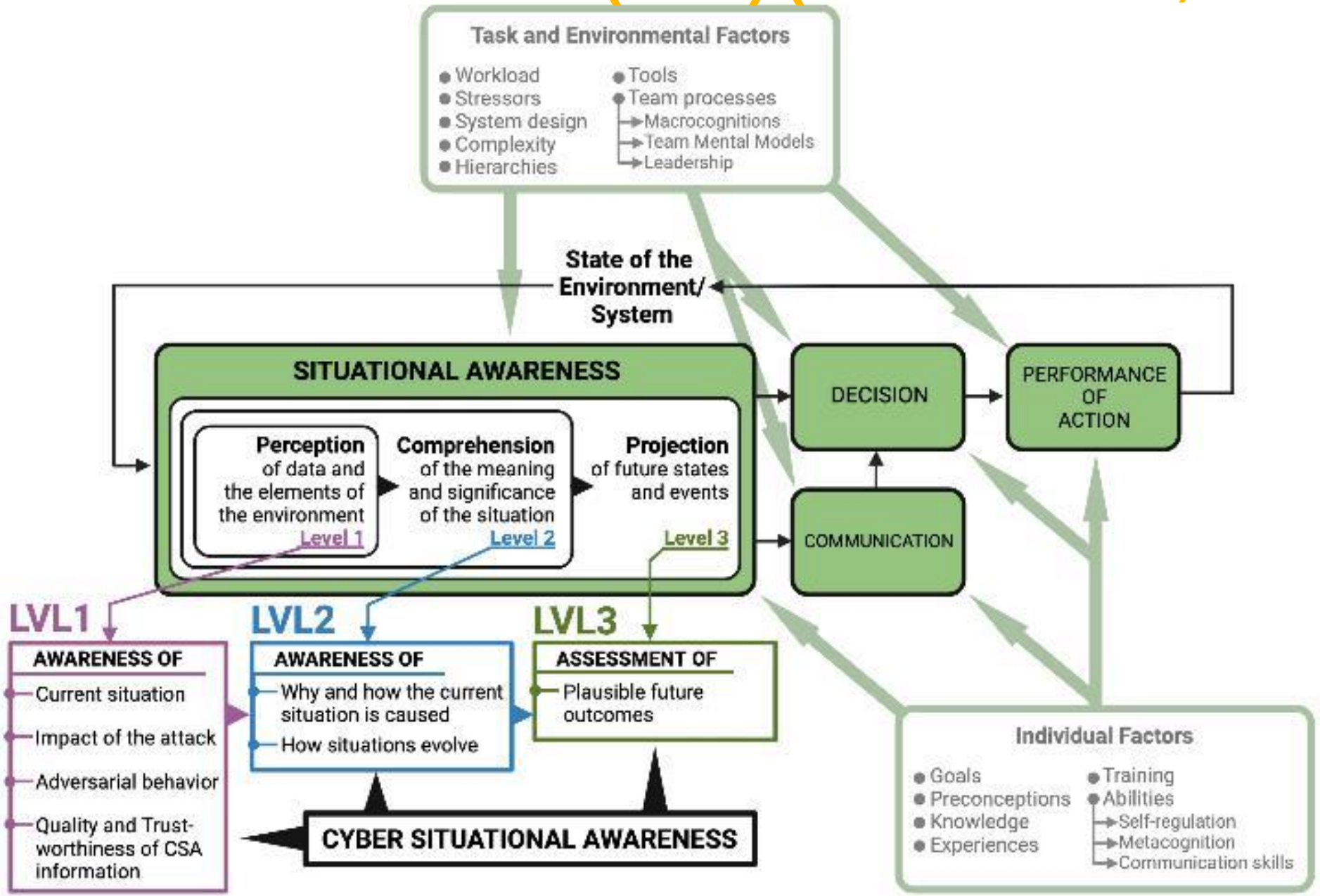
(very) little examples

Psychological and Social Factors in Energy Sector Cybersecurity

Understanding Human Psychology

- Cognitive biases and their impact on cybersecurity.
- Psychological theories relevant to cybersecurity behaviour.
- Designing cybersecurity systems with human psychology in mind.
  - Situational Awareness (Endsley, 1998)
- An interface redesign that reduced user errors based on psychological research.

Cyber situational awareness (CSA) (Barford et al., 2009)



Psychological and Social Factors in Energy Sector Cybersecurity

Social Dynamics and Cybersecurity

- Influence of social norms and peer behaviour on individual cybersecurity practices.
- The role of leadership in fostering a security-conscious culture.
  - Role Modelling (Bandura, 1988)
- Social factors in cybersecurity training and awareness programs.

Psychological and Social Factors in Energy Sector Cybersecurity

Enhancing Security Through Psychology

- Psychological strategies to increase security protocol adherence.
- Behavioural change techniques applied to cybersecurity.
- The role of motivation and rewards in enhancing cybersecurity behaviours.
- Real-world example: A rewards program that successfully increased cybersecurity vigilance among engineers.
- Future BCT using AI

Psychological and Social Factors in Energy Sector Cybersecurity

Addressing Social Engineering Threats

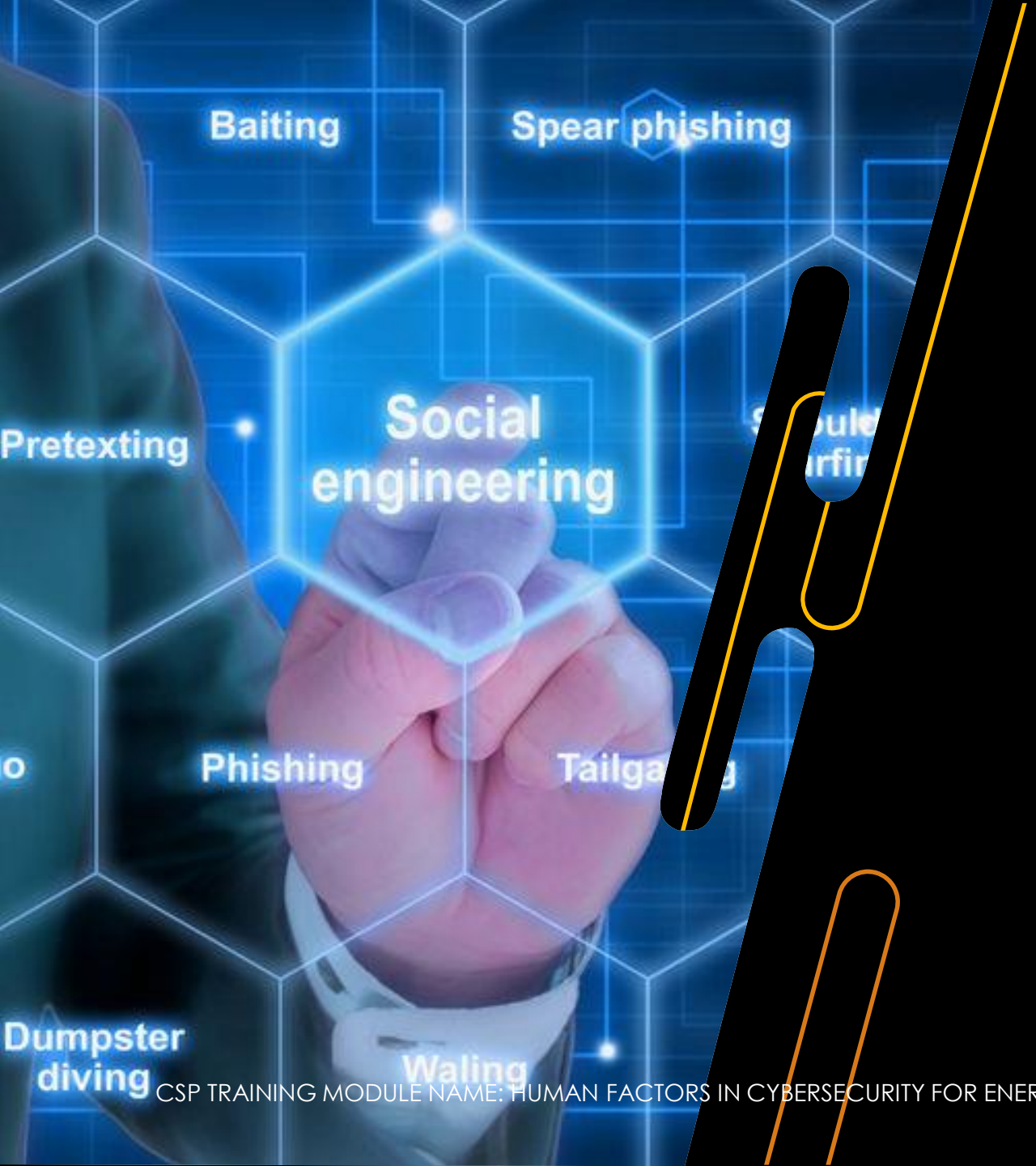
- Understanding social engineering tactics from a psychological perspective.
- Training personnel to recognize and respond to social engineering attacks.
- Building a culture of scepticism, vigilance and verification.
- Real-world example: A company's response to a spear-phishing campaign targeting executives.

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

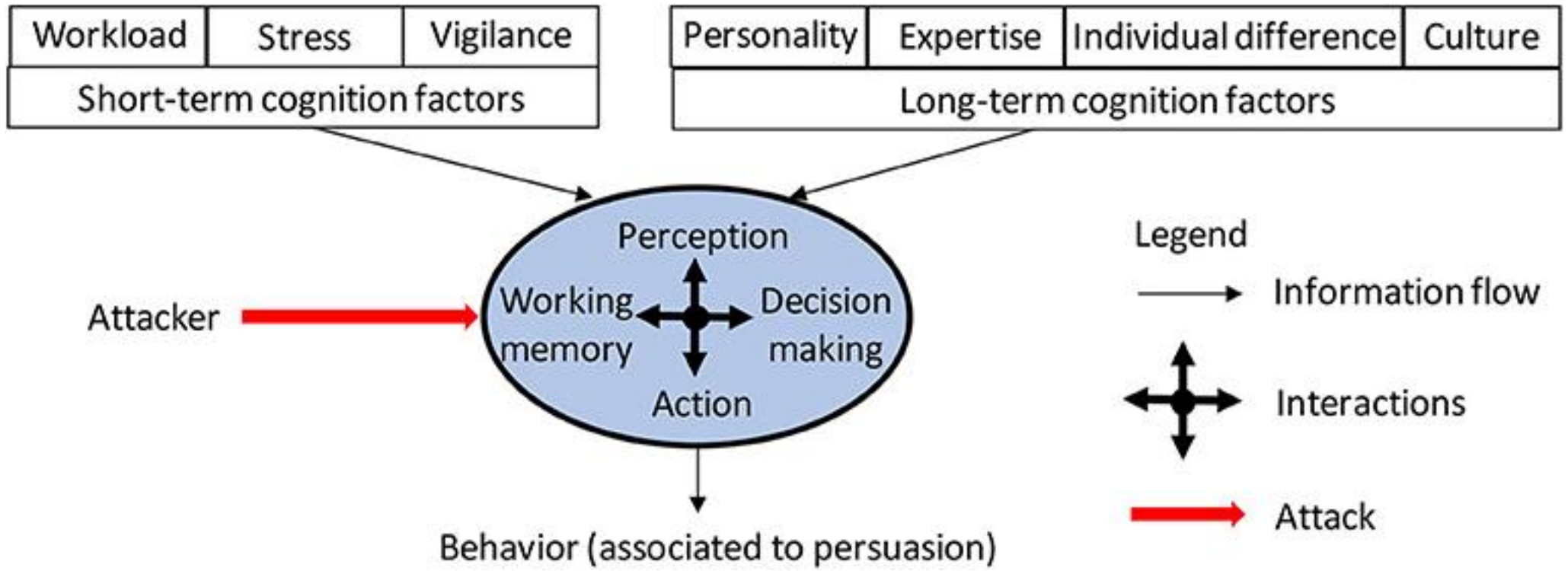


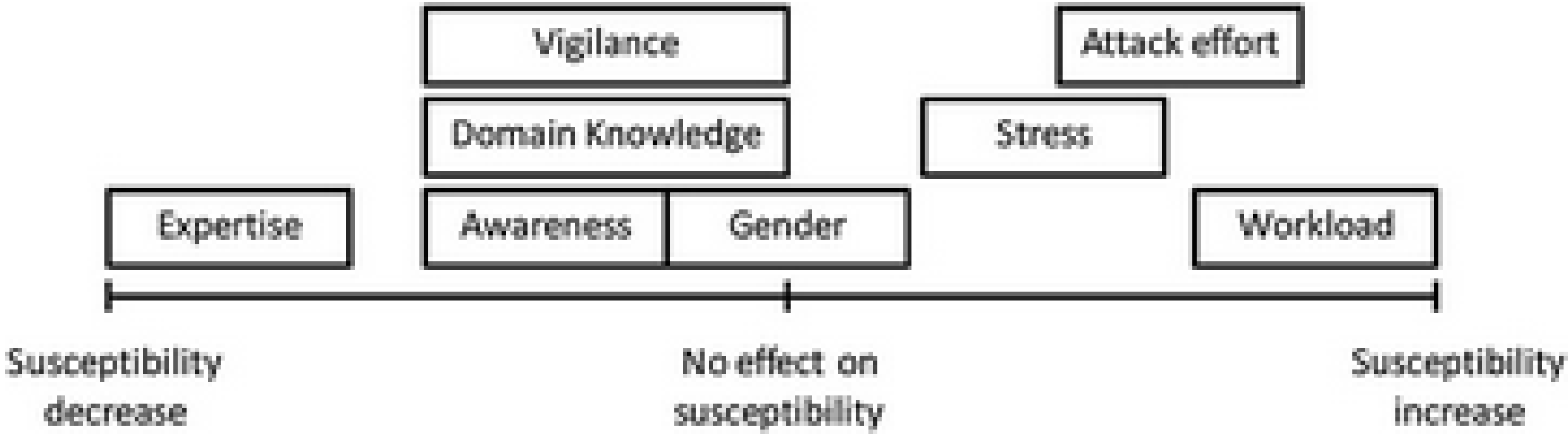
Human Vulnerabilities in Energy Sector Cybersecurity

Identifying Human Vulnerabilities

- Common human vulnerabilities in energy sector cybersecurity contexts.
- The role of user behaviour analytics in identifying risky behaviours.
- Strategies for mitigating human vulnerabilities.
- Real-world example: Incident involving an exploited vulnerability due to poor password practices.

Cogntive exploits and attack vectors




Vigilance
Attack effort
Domain Knowledge
Stress
Expertise
Awareness
Gender
Workload
Susceptibility decrease
No effect on susceptibility
Susceptibility increase

9 Different Types of Phishing

- Email phishing
- Spear phishing
- Whaling
- Smishing
- Vishing
- Crypto phishing
- Watering hole attacks
- Malvertisements
- Angler phishing

10 Tips to Protect Yourself Against Phishing

- Hover over links to preview the URL before clicking
- Verify email addresses
- Use reputable security software
- Enable two-factor authentication (2FA)
- Avoid pop-ups
- Be cautious with personal info
- Verify requests for money
- Use strong passwords
- Avoid using public networks
- Report suspected scams

Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior

Abstract

There is interest in better und
ultimately impacted by their
perceived and how someone
framework for explaining this
victimization is essential to u
human despite increased relia
and in real time yet are still in
attitudes and behaviors that
students sampled from two pu
the Online Security Behavior
with an index of perceived vu
regression indicated subscale
competent enough to underst
resulting from a social desira
that knowledge is an essential
vulnerability may depend upo

Keywords: cybersecurity, pe

What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context

Lies De Kimpe [a], Michel Walrave [a], Pieter Verdegem [b] and Koen Ponnet [a,c]

[a]Department of Communication Studies, University of Antwerp Antwerp, Belgium; [b]Communication and Media Research Institute (CAMRI), University of Westminster, Northwick Park, UK.; [c]Department of Communication Studies, imec-mict-Ghent University Ghent, Belgium

ABSTRACT

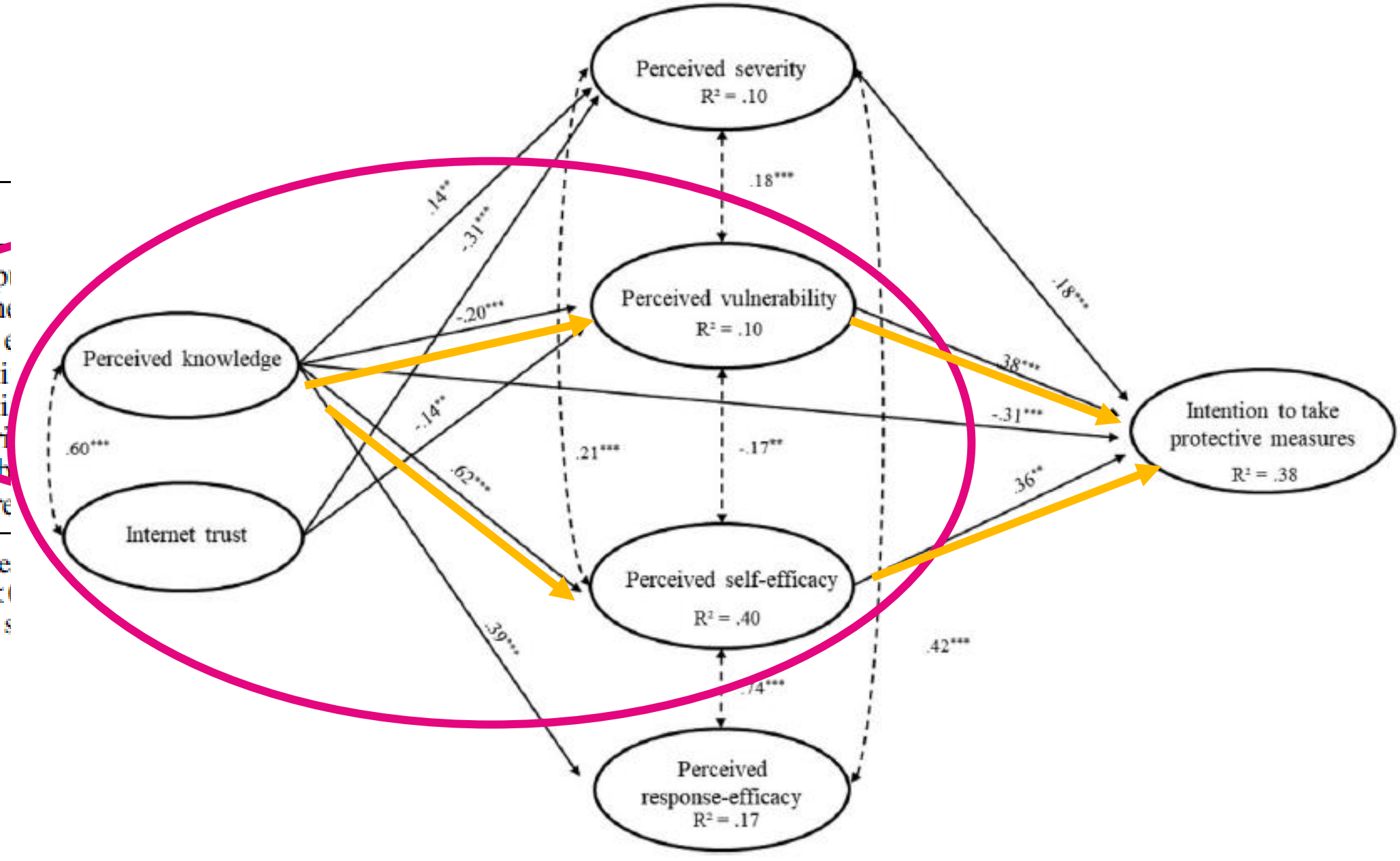
Individual internet users are commonly considered the weakest links in the cybersecurity chain. One reason for this is that they tend to be overoptimistic regarding their own online safety. To gain a better understanding of the cognitive processes involved in this assessment, the current study applies an extended version of the protection motivation theory. More specifically, this study includes perceived knowledge and internet trust to discover how these antecedents influence the threat and coping appraisal processes. Based on representative survey data collected from 967 respondents, we found that people who feel well-informed about online safety feel less vulnerable to cybercrime and are less inclined to take security measures. At the same time, feeling informed is associated with being more convinced of the severity of cybercrime. High levels of trust in the safety of the internet are linked to the feeling that one is less vulnerable to cybercrime and the perception that cybercrime is not a severe threat. Future interventions should remind internet users about their own perceived vulnerability and the risks that exist online while ensuring that internet users do not lose their trust in the internet and confidence in their own online knowledge.

ARTICLE HISTORY

Received 12 February 2019
Accepted 25 February 2021

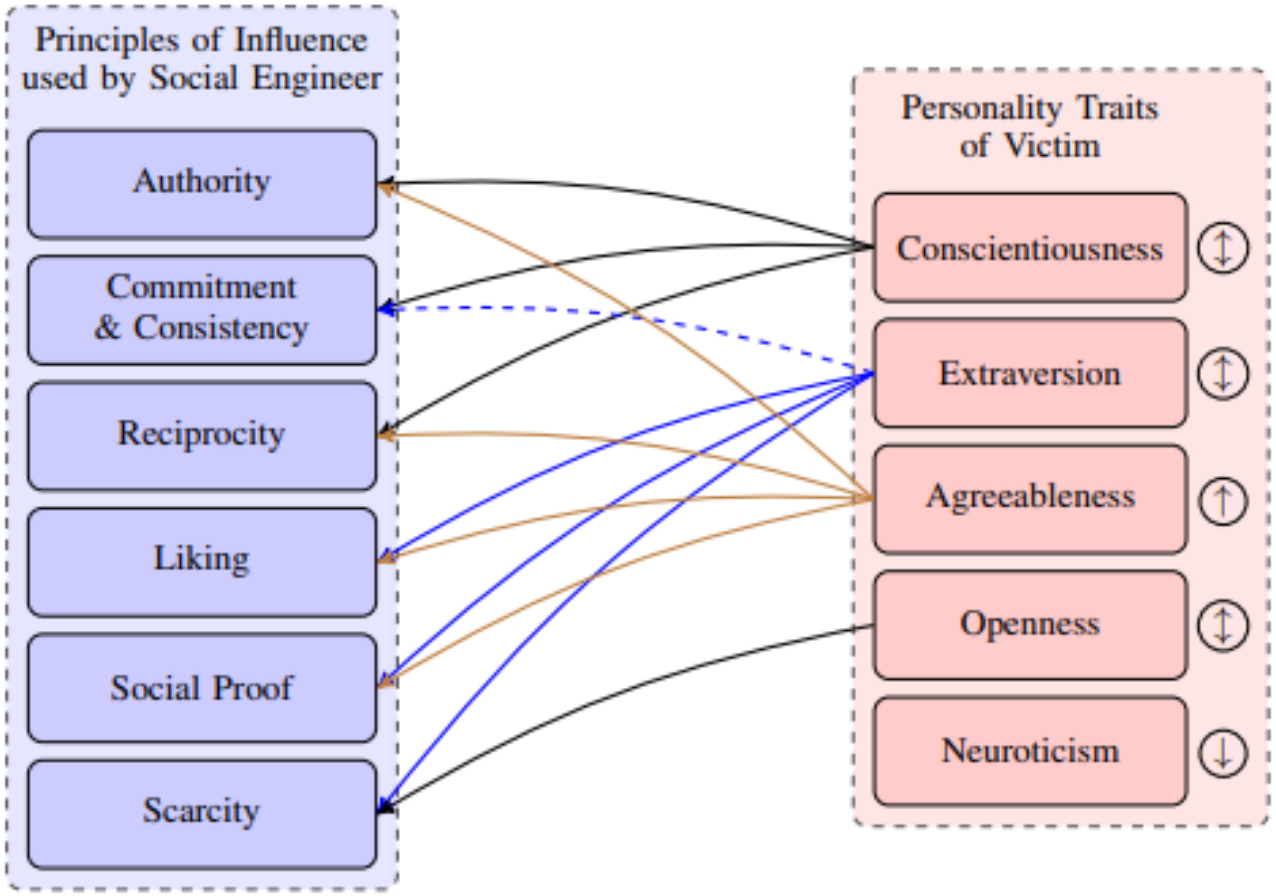
KEYWORDS

Protection motivation theory; cybercrime; optimism bias; perceived knowledge; internet trust


Perceived severity
R² = .10
Perceived vulnerability
R² = .10
Perceived knowledge
Internet trust
Perceived self-efficacy
R² = .40
Perceived response-efficacy
R² = .17
Intention to take protective measures
R² = .38
.14**
-.31***
.18***
-.18***
-.20***
.38***
-.31***
.60***
-.14**
.21***
-.17**
.62***
.36**
.39***
.42***
.74***

Social Engineering Personality Framework (SEPF)

- Attack:
- C: rules
- E: Excitement
- A: Many ways in…
- O: Scarcity - restrict freedom
- N: Protective



Profiles

Motivations:

1. **Financial Gain**: Many attackers are motivated by financial incentives
2. **Hacktivism**: Some attackers engage in cyberattacks to promote a social or political agenda, often using digital means to make a statement.
3. **Curiosity**: Curiosity-driven attackers, often referred to as "script kiddies," explore vulnerabilities for the thrill of it
4. **Espionage**: State-sponsored attackers or cyber spies aim to gather intelligence, classified information, or trade secrets.

Psychological Characteristics:

1. **Anonymity**
2. **High Intelligence**
3. **Risk-Taking**
4. **Lack of Empathy**

Attack Techniques:

1. **Phishing**: Attackers often use social engineering techniques to trick individuals into revealing sensitive information or clicking on malicious links.
2. **Malware**: Attackers deploy various types of malicious software, like viruses, worms, and Trojans, to compromise systems and steal data.
3. **Advanced Persistent Threats (APTs)**: State-sponsored attackers employ APTs to infiltrate and maintain long-term access to target systems discreetly.

Psychological Factors:

1. sense of power and control when successfully breaching systems, leading to a cycle of addiction to cybercrime.
2. justify their actions by believing they are exposing vulnerabilities or fighting for a cause they deem just.

Human Vulnerabilities in Energy Sector Cybersecurity

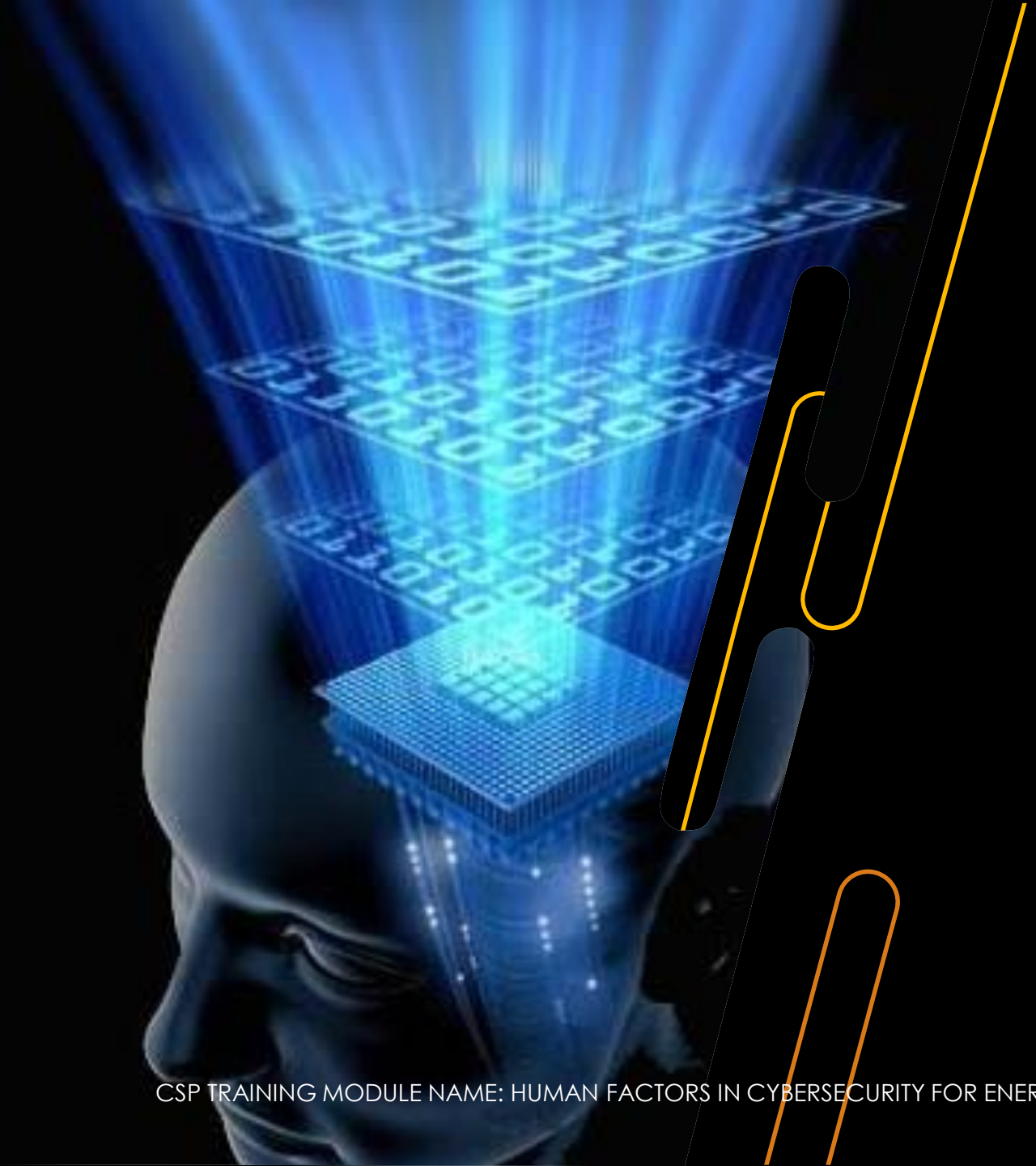
Impact of Human Error

- Types of human errors and their consequences for cybersecurity.
- Methods for reducing errors, such as simplification of systems and processes.
- Importance of error reporting and management systems.
- ENISA

Human Vulnerabilities in Energy Sector Cybersecurity

Training to Reduce Human Error

- Role of targeted training programs in addressing specific human vulnerabilities.
- Simulation
- Gamification
- Scenario based learning
- Continuous learning
- The importance of simulation and drills in reinforcing correct behaviours.
- Continuous improvement of training programs based on incident feedback.

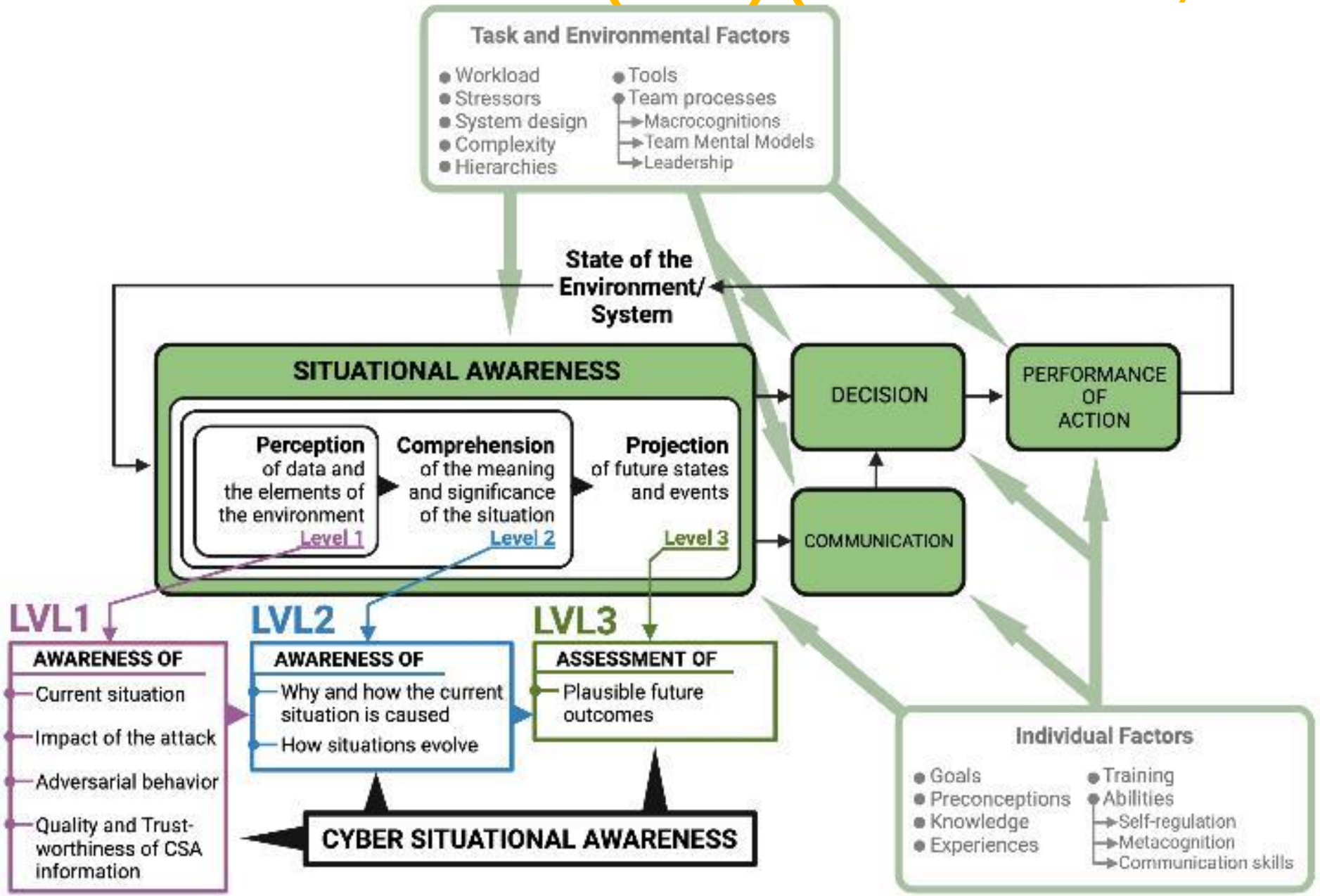


Human Vulnerabilities in Energy Sector Cybersecurity

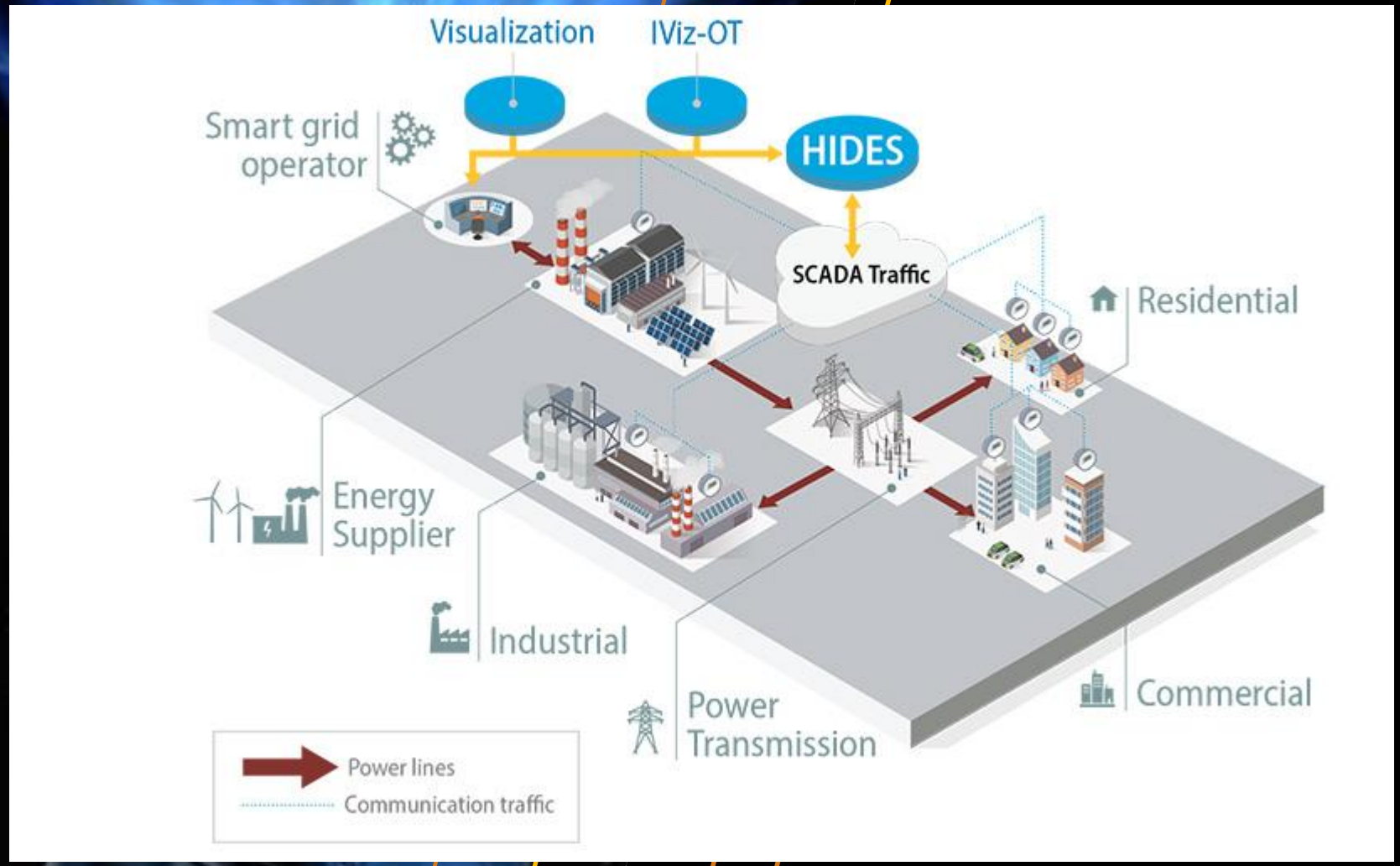
Enhancing Situational Awareness

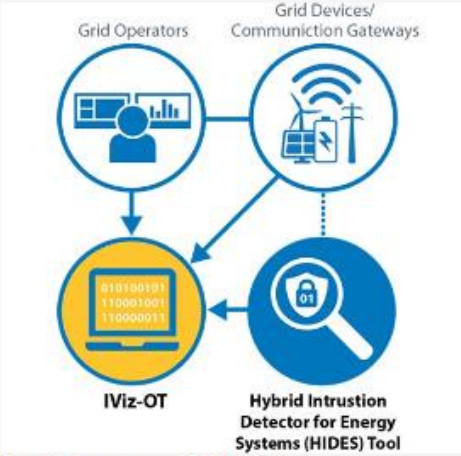
- Importance of situational awareness in preventing human errors.
- Endsly
- Perception
- Comprehenssion
- Projection
- Tools and technologies to support situational awareness in cybersecurity.
- Adapeted viualisations
- Integrating situational awareness into daily operations and decision-making.

Cyber situational awareness (CSA) (Barford et al., 2009)



Enhancing Situational Awareness





Key Features of IViz-OT:

- Visualizes alerts to support situational awareness for grid operators
- Maps alerts to possible scenarios
- Customized application programming interface (API) and supports the integration of alert scenarios and databases
- Compatible with vendor devices.

Key Features of HIDES:

- Detects both IT- and SCADA-specific attacks
- Aggregates data to integrate cyber logs and grid information
- Visualizes grid on the dashboard to provide situational awareness.

Organizational Culture, Communication, and Cybersecurity

Role of Organizational Culture

- Definition and impact of organizational culture on cybersecurity.
- Characteristics of a strong cybersecurity culture.
  - Values (Lencioni, 2002)
  - Adherence and compliance
- Strategies for cultivating a positive cybersecurity culture.
  - Psychological Safety in the Workplace

Organizational Culture, Communication, and Cybersecurity

Effective Cybersecurity Communication

- Principles of effective communication in cybersecurity.
- Overcoming barriers to effective cybersecurity communication.
- Role of transparent communication in incident response.
- Post cybersecurity incident

Organizational Culture, Communication, and Cybersecurity

Leadership in Cybersecurity Culture

- Building cybersecurity leadership at all levels of the organization.
  - Vertically AND horizontally

Organizational Culture, Communication, and Cybersecurity

Fostering Collaboration and Trust

- Defining Collaboration and Trust: *Collaboration in the* energy sector *involves the sharing of information, resources, and best practices to enhance collective cybersecurity defenses. Trust underpins these collaborative efforts, ensuring that shared information is reliable and that partners will act responsibly with shared data and insights*.
- Importance of trust and collaboration in cybersecurity efforts.
  - Information Sharing
  - Joint Cybersecurity exercises
- Techniques for building trust within and across teams.
  - Alliances, partnerships
- Collaborative approaches to cybersecurity problem-solving.
- Real-world example: Cross-departmental collaboration project that strengthened overall cybersecurity posture.

Communication and Collaboration Across Domains

Cross-Domain Cybersecurity Challenges

- Challenges and opportunities in cross-domain cybersecurity collaboration.
- Importance of interoperability and shared standards.
- ENISA, NIS 2
- Strategies for effective cross-domain communication.

Communication and Collaboration Across Domains

Building Collaborative Networks

- The role of professional networks and alliances in enhancing cybersecurity.
- Benefits of public-private partnerships in cybersecurity initiatives.
- ESCO
- Leveraging expertise across domains for comprehensive cybersecurity solutions.

Communication and Collaboration Across Domains

Collaborative Incident Response

- Principles of collaborative incident response planning.
- Importance of clear roles and communication channels during incidents.
- Benefits of joint exercises and simulations.
- Decision-making under pressure
- Cultural aspects
- Locked-Shields and Energy Sector

Communication and Collaboration Across Domains

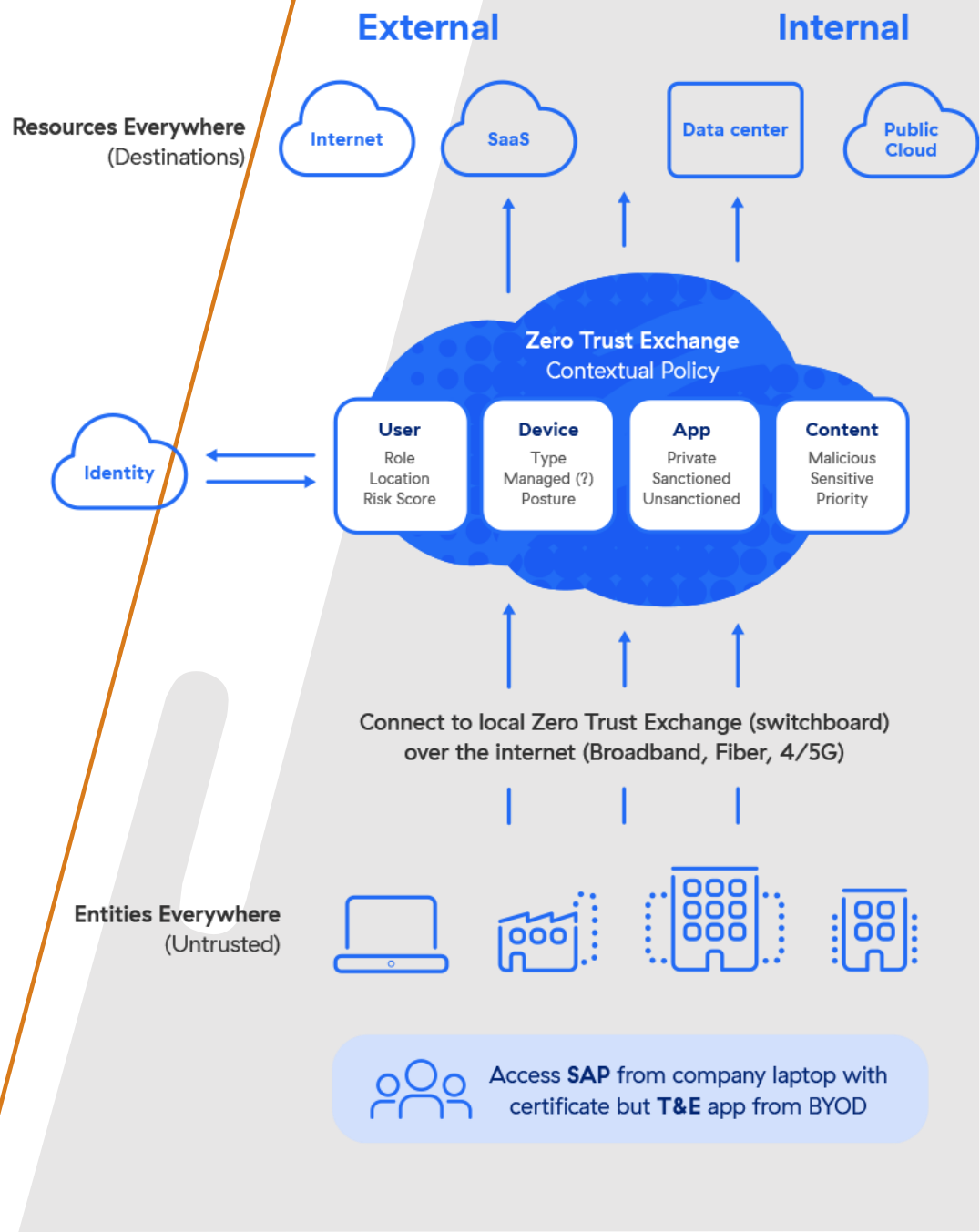
Overcoming Barriers to Collaboration

- Common barriers to effective cybersecurity collaboration and how to overcome them.
- The role of trust and transparency in collaborative efforts.
- Best practices for sustaining long-term collaborative relationships.

Decision Making at Strategic, Operational, and Tactical Levels

Strategic Decision Making

- Overview of strategic decision-making in energy sector cybersecurity.
- Long-term planning and policy development for robust cybersecurity frameworks.
- Integration of cybersecurity into overall business strategy.
- Real-world example: An energy sector company's strategic decision to adopt a zero-trust architecture.



Decision Making at Strategic, Operational, and Tactical Levels

Operational Decision Making

- Role of operational decisions in maintaining day-to-day cybersecurity.
- Operational responses to identified threats and vulnerabilities.
- Coordination between cybersecurity teams and other operational units.
- Real-world example: An operational decision to isolate a compromised system in a plant, preventing a wider breach.

Decision Making at Strategic, Operational, and Tactical Levels

Tactical Decision Making

- Nature of tactical decisions in responding to immediate cybersecurity threats.
- Tools and techniques for effective tactical decision-making, including incident response teams and real-time threat intelligence.
- Importance of agility and flexibility in tactical decisions.
- Real-world example: Rapid tactical response to a ransomware attack on a management system.

Decision Making at Strategic, Operational, and Tactical Levels

Integrating Decision Levels

- Ensuring coherence and alignment between strategic, operational, and tactical decision-making levels.
- Mechanisms for feedback and learning across decision-making levels.
- Role of leadership in bridging gaps between different decision-making levels.
- Real-world example: Integrated decision-making framework that enabled a seamless response to a coordinated cyber-physical attack.

Training, Awareness, and Communication Programs for Energy Sector Personnel

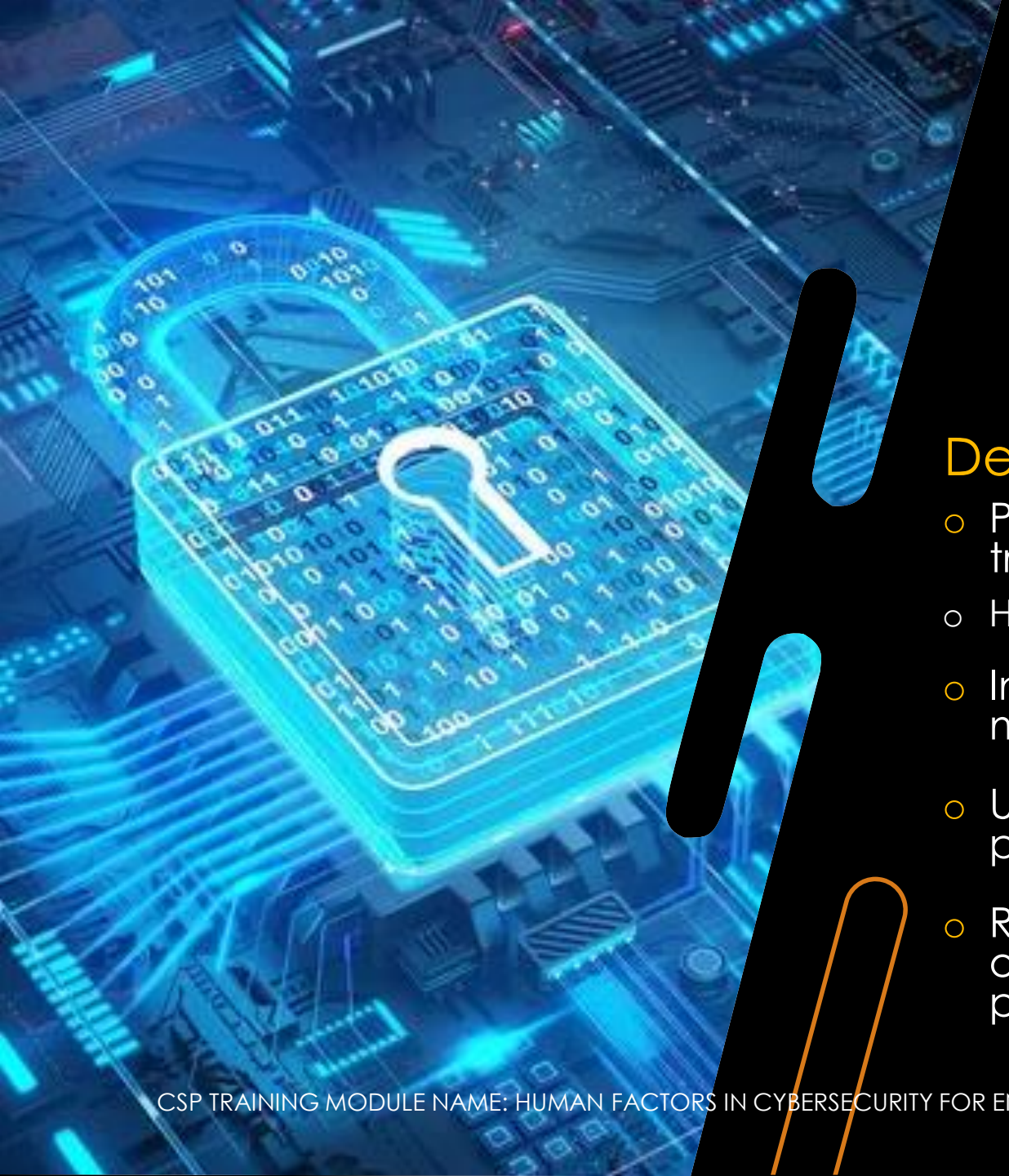
Importance of Training and Awareness

- The critical role of continuous training and awareness in energy sector cybersecurity.
- Elements of effective cybersecurity training programs for personnel.
- The impact of awareness programs on reducing human error and enhancing security culture.
- , NIS 2

Training, Awareness, and Communication Programs for Energy Sector Personnel

Enhancing Communication for Cybersecurity

- Best practices for communicating cybersecurity policies and incidents to energy sector personnel.
- The role of clear, consistent communication in fostering a proactive cybersecurity stance.
  - Clear Messaging
  - Timely Information Flow
  - Actionable Intelligence
- Strategies for overcoming communication barriers in diverse and dynamic energy sector environments.
  - Multichannel communication
  - Feedback



Training, Awareness, and Communication Programs for Energy Sector Personnel

Designing Effective Training Programs

- Principles for designing engaging and impactful training programs.
- Habits, Self-efficacy, Metacognition
- Incorporating adult learning theories and methodologies in cybersecurity training.
- Use of simulations and drills in reinforcing learning and preparedness.
- Real-world example: A energy sector academy's use of VR simulations to train cadets on cybersecurity protocols.

Future Trends, Challenges, and the Role of Communication

Emerging Cybersecurity Trends

- An overview of emerging trends in cybersecurity, including AI, machine learning, and IoT.
- The implications of these trends for energy sector cybersecurity strategies.
- Preparing for future cybersecurity challenges through innovation and adaptability.
- Real-world example: Adoption of AI-based threat detection systems on smart ships.

Future Trends, Challenges, and the Role of Communication

Addressing Future Cybersecurity Challenges

- Anticipating and mitigating new types of cyber threats in the energy sector.
- The importance of staying ahead of the curve through research and collaboration with cybersecurity experts.
- Challenges posed by the increasing complexity and connectivity of energy sector operations.

Future Trends, Challenges, and the Role of Communication

The Evolving Role of Communication

- The critical role of effective communication in addressing future cybersecurity challenges.
- Enhancing cross-sector and cross-border communication for a unified response to cyber threats.
- Leveraging new communication technologies and platforms for better threat intelligence sharing.
- Real-world example: Iviz-OT.

Future Trends, Challenges, and the Role of Communication

Preparing for the Future

- Strategic planning and investment in cybersecurity capabilities to prepare for future challenges.
- The role of leadership in fostering a forward-looking cybersecurity culture.
- Importance of global cooperation and information sharing in strengthening energy sector cybersecurity resilience.
- Industrial Automation and Control Systems (IACS)

Please evaluate

https://forms.gle/uTSmjnuBKU2o4Uiy9

Choose: **CSP002_S_E: Human Factors and Energy Cybersecurity**

Resources: Books and Reference Materials

1. "European Cybersecurity Skills Framework": European Union Agency for Cybersecurity (ENISA) Publication
2. European Union Agency for Cybersecurity (ENISA). (2019). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. Retrieved from https://www.enisa.europa.eu.
3. Hanzu-Pazara, R., Raicu, G., & Zăgan, R. (2019). The Impact of Human Behaviour on Cyber Security of the Maritime Systems. Advanced Engineering Forum, 34, 267-274.
4. Wiederhold, B. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior, and Social Networking, 17(3), 131-132.
5. Aşan, C. (2023). The Role of Cyber Situational Awareness of Humans in Social Engineering Cyber Attacks on the Maritime Domain. Mersin University Journal of Maritime Faculty. Link
6. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. Network, 2, 123-138.
7. Endsley, M. R., & Jones, D. G. (2024). Situation Awareness Oriented Design: Review and Future Directions. International Journal of Human–Computer Interaction, 1-18.
8. Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Social Psychology: An Under-used Tool in Cybersecurity.
9. Knox, B. J., Lugo, R. G., & Sütterlin, S. (2019). Cognisance as a human factor in military cyber defence education. IFAC-PapersOnLine, 52(19), 163-168.

Thank you

Please send any questions to:
Ricardo.Lugo@taltech.ee

CyberSecPro