

Cibersegurança: O Papel Essencial do Fator Humano

Miriam von Zuben

Analista de Segurança
CERT.br/NIC.br

Live Intrade Rede – Ceptro.br/NIC.br
Evento *Online* – 14 de outubro de 2026

cert.br nic.br cgi.br

Desmistificando o Elo mais Fraco

1. The Persistent Myth of the “Human is Weakest Link”

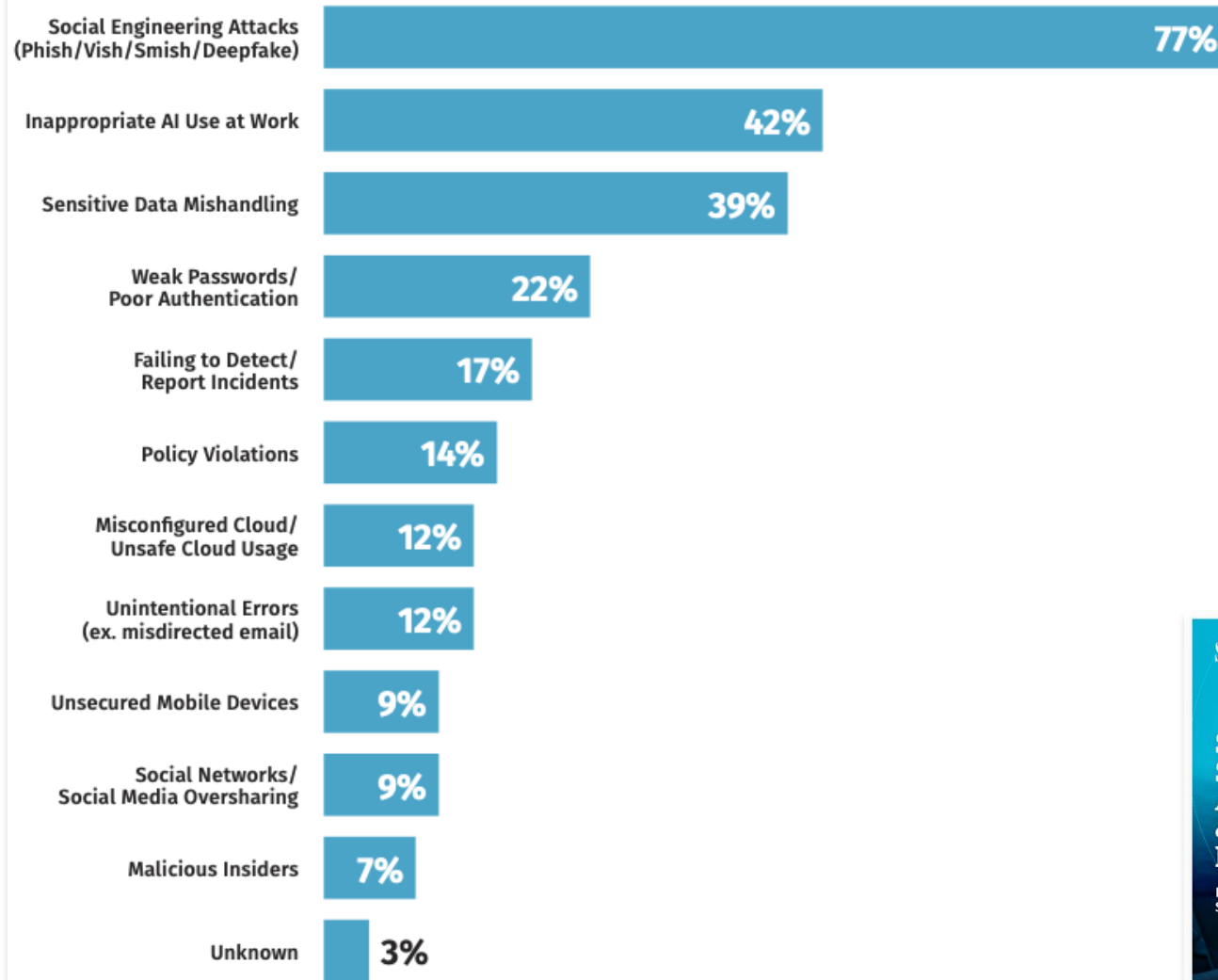
When an employee causes an incident, from falling victim to a phishing attack to accidentally sharing sensitive data in the cloud, far too often leaders perceive this as “the human is the weakest link.” However, people are not the problem but, the environments we create are.

Security policies, tools, and expectations have become incredibly confusing, difficult and overwhelming for people. Yes, security is simple for most security professionals, but we live and breathe security daily.

People want to do the right thing, it's just that we have done a terrible job of communicating security in simple terms and making security as easy as possible. This is why people are not the weakest link; **they are the primary attack vector**. When people do cause an incident, instead of blaming them, we should be looking at the environment we have created and ask ourselves what we can do differently.

Top Human Risks (Your Risk Focus)

Breakdown showing what percentage of respondents selected a given option as their top areas of risk focus for 2026.



<https://www.sans.org/for-organizations/workforce/resources/security-awareness-report>

Fortalecendo o Elo Humano

"Users are not the enemy.

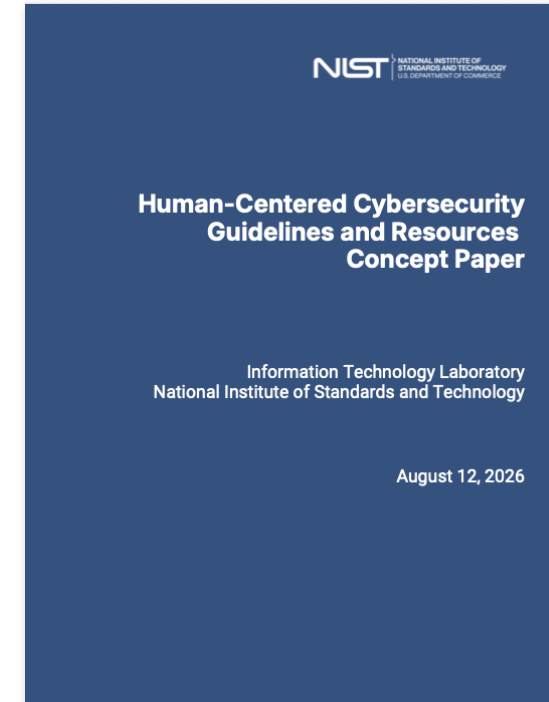
***They want to do their jobs,
and they want to do them securely***

***- if the security mechanisms do not make it
impossible for them to work."***

Anne Adams & M. Angela Sasse, 1999

Mudança de Paradigmas

- Do tecnocentrismo:
 - pessoas como vetor de risco
 - abordagem punitiva
 - fadiga de alertas e sobrecarga de decisões
 - conscientização via longos treinamentos anuais
- À segurança centrada no humano (HCC):
 - pessoas como “primeira linha” e “sensor ativo” de defesa
 - maiores esforços em investigar as causas dos problemas e melhorar os sistemas
 - segurança *by design*, com configurações *default* mais seguras
 - orientações mais curtas, contextualizadas e oportunas
 - gamificação e atividades práticas para estimular engajamento e aprendizagem



<https://csrc.nist.gov/projects/human-centered-cybersecurity/human-centered-cybersecurity-concept-paper>

SIM3: O Fator Humano na Maturidade de um CSIRT

 Open CSIRT Foundation

SIM3 v2 interim Self Assessment Tool

Open CSIRT Fo

Organisation Human Tools Processes

With **Humans** we refer to the people working together to provide the services described in the Organisation area and satisfy the mandate. All people contributing to the goals of the (CSIRT) organisation that manages security incidents, require a technical and/or management oriented education with considerable on-the-job training plus additional training for more detailed expertise like malware analysis or forensics. The 'H' Parameters in this area are about the factors of importance in regard the most

The 'H' Parameters in this area are about the factors of importance in regard the most important factor in any CSIRT: the human 'capital' of the people working there.

H-1 : Code of Conduct/Practice/Ethics

H-2 : Staff Resilience

H-3 : Skillset Description

H-4 : Staff Development

H-5 : Technical Training

H-6 : Soft Skills Training

H-7 : External Networking

<https://sim3-check.opencsirt.org/>

Mitigando *Insider Threats*

Definições SEI/CERT

*“A **malicious insider threat** is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems”, 2012*

*“**Insider Threat** - the potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization”, 2017*

*“**Insider Risk** - the impact and likelihood associated with the realization of an insider threat”, 2026*

<https://www.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/>
https://www.sei.cmu.edu/documents/5777/5692_CSG_Book_20-optimized.pdf

Definições CISA

“An insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, negligent, or unintentional acts that negatively affect the confidentiality, integrity, and availability of the organization, its data, personnel, facilities, and/or associated resources.”, 2026

“An insider is any person who has or had authorized access to or knowledge of an organization’s resources, including personnel, facilities, information, equipment, networks, and systems. An insider may be:”



A person the organization trusts and to whom the organization has provided sensitive information and access. This can include both full and part-time employees, contractors, and external third parties who still have some level of access



A person with regular or intermittent access to facilities and/or networks

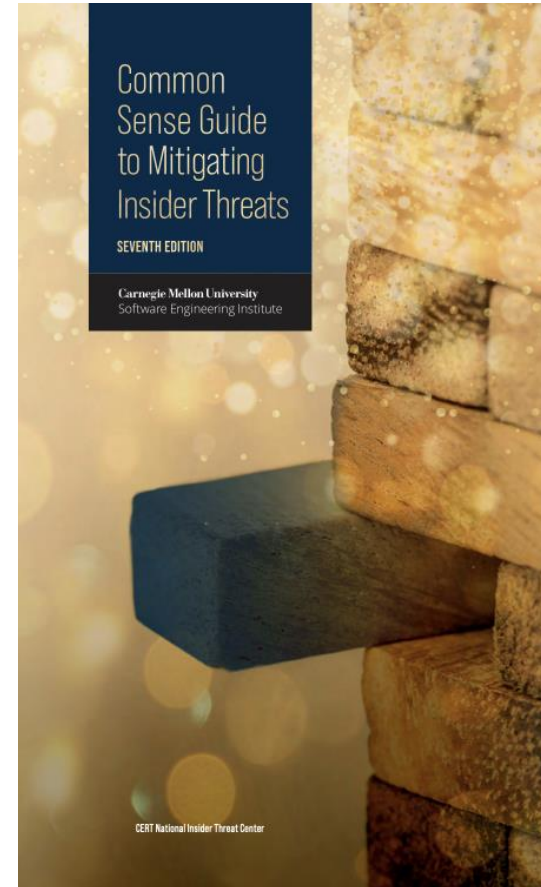
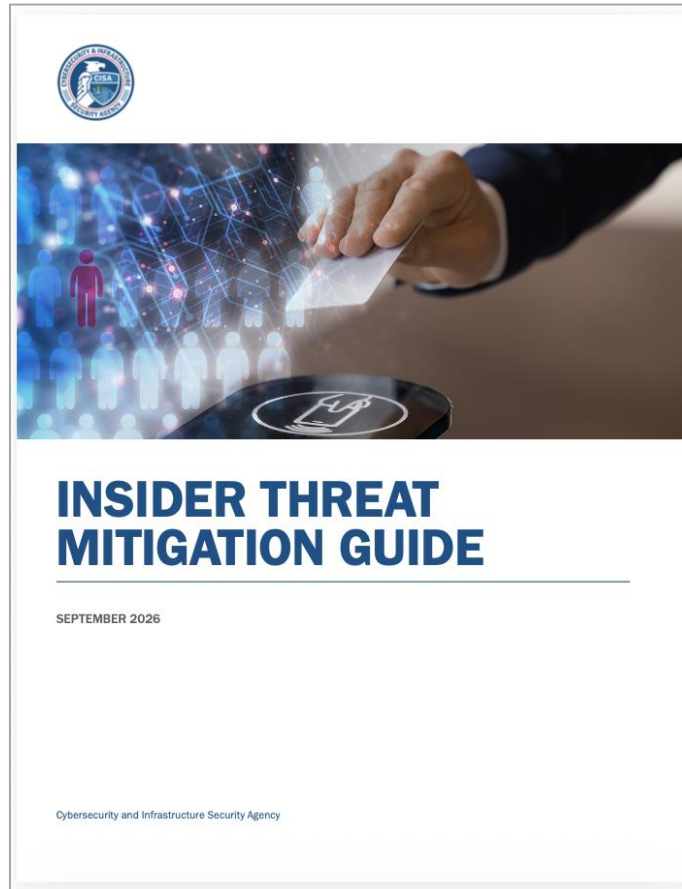


A person who develops the organization’s products and services, including those who know the sensitive details of the products that provide value to the organization



A person who is knowledgeable about the organization’s fundamentals, including pricing, costs, and its strengths and weaknesses, and/or the organization’s business strategy and goals

Insider Threat Mitigation Guides



<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>

<https://www.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/>

Novos Desafios

Insider Threats e IA

Novos Desafios - *Insider Threats* e IA

Alignment

Agentic misalignment: How LLMs could be insider threats

Jun 20, 2025

The Agentic Insider: Redefining Insider Threats Beyond Human Actors in Autonomous AI Systems

Christian Kengne
Polytechnique Montréal
GIGL (Génie informatique et Génie logiciel)
Montréal, Quebec, Canada
christian.kengne@polymtl.ca

<https://www.anthropic.com/research/agentic-misalignment>

<https://dl.acm.org/doi/epdf/10.1145/3774905.3795476>

***“People are not the problem but,
the enviroments we create are.”***

Lance Spitzner

<https://www.sans.org/blog/why-leadership-still-misunderstands-human-risk>

Obrigada!

© para materiais de conscientização: doc@cert.br

© notificações para: cert@cert.br

X @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br