University of Applied Sciences and Arts Northwestern Switzerland
School of Business

member of swissuniversities

AACSB ACCREDITED

MSc Blockchain
Spring Semester 2026

Lecture 1
Cybersecurity Management I/II

Module
Cybersecurity and Cryptography

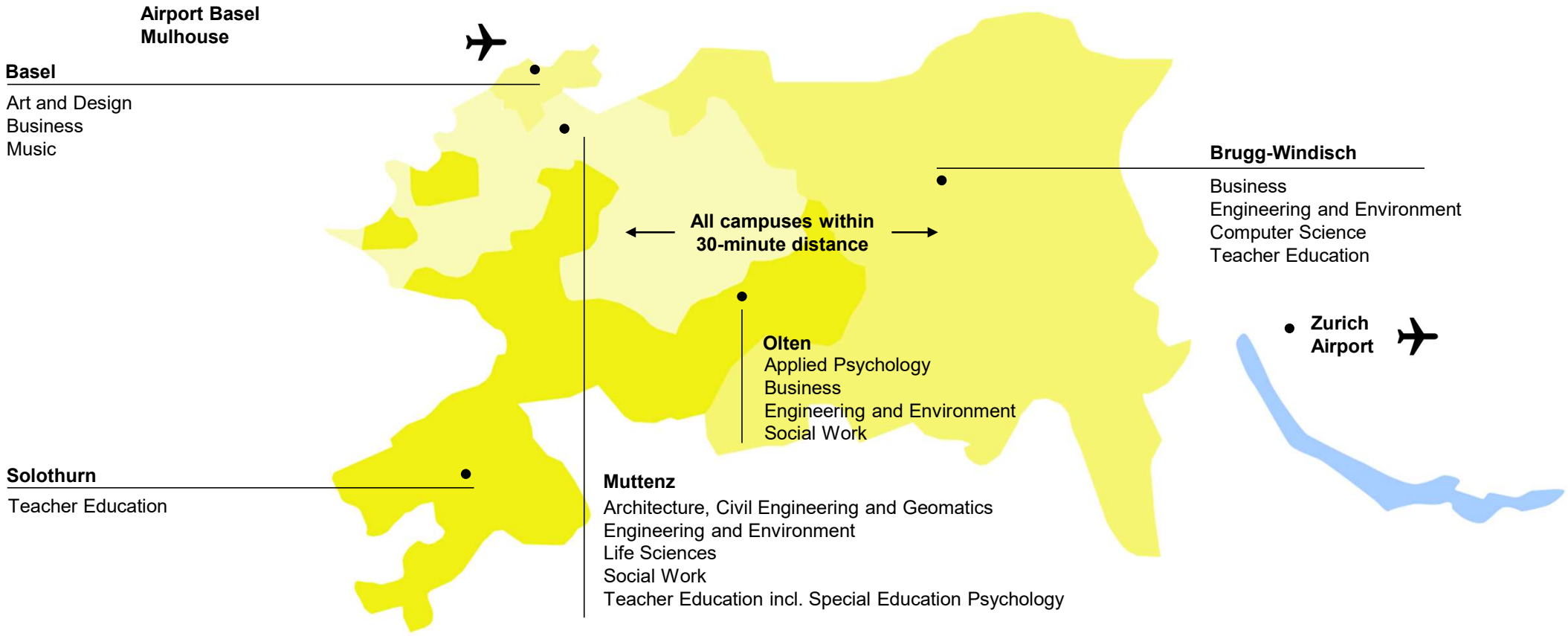
Prof. Dr. Bettina Schneider
Head of Competence Center Digital Trust
Institute for Information System
FHNW School of Business

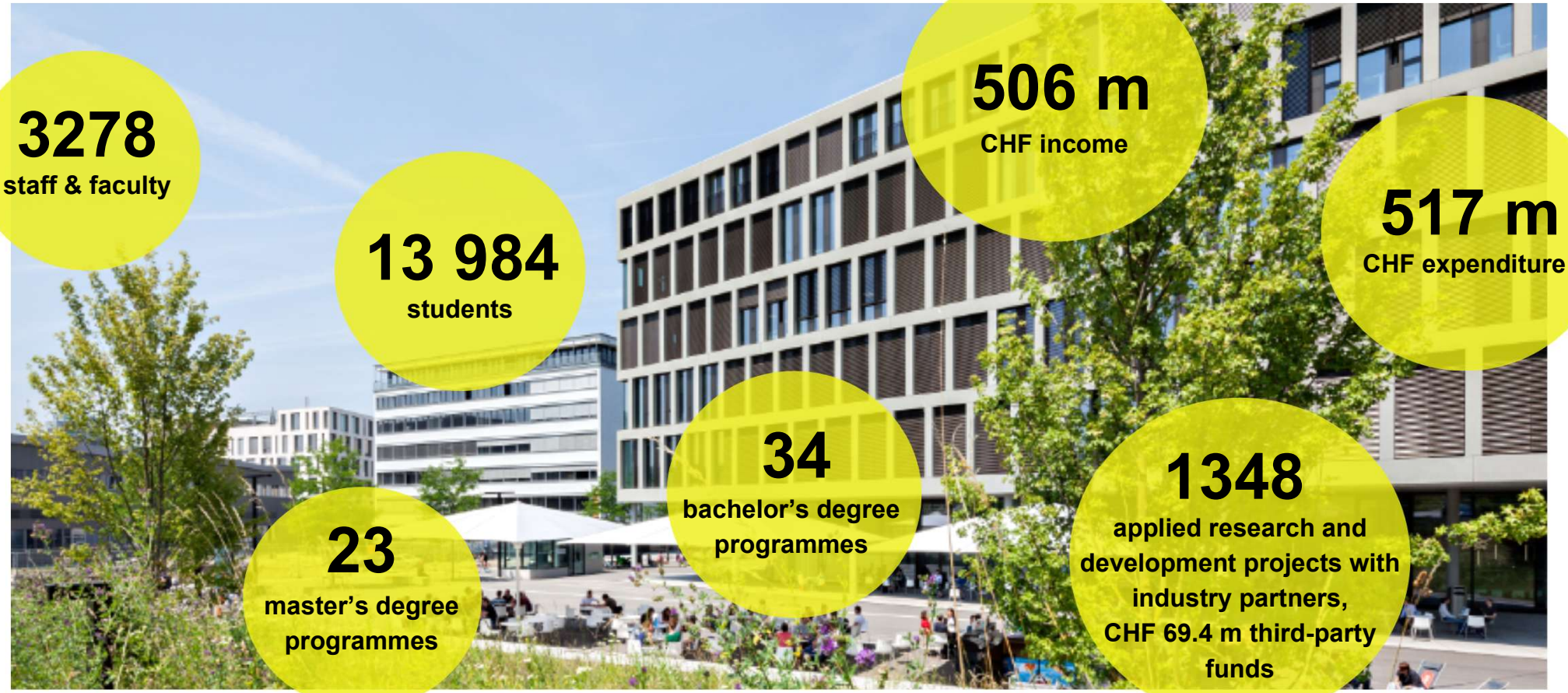
slide-deck based on lecture from Hermann Grieder

May 2026

Course Introduction

FHNW University of Applied Sciences and Arts Northwestern Switzerland




3278
staff & faculty
13 984
students
506 m
CHF income
517 m
CHF expenditure
34
bachelor's degree programmes
23
master's degree programmes
1348
applied research and development projects with industry partners, CHF 69.4 m third-party funds

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

member of swissuniversities

AACSB ACCREDITED

Engineering and Environment

Applied Psychology

Business

Art and Design

Life Sciences

Teacher Education

Computer Science

Architecture, Civil Engineering and Geomatics

Music

Social Work

Obligatory Mandate

The Team of Digital Trust

Prof. Dr. Petra Maria Asprion

Head
Digital Trust

Prof. Dr. Bettina Schneider

Head
Digital Trust

Prof. Dr. Walter Dettling

Senior
Researcher &
Lecturer

Prof. Dr. Barbara Eisenbart

Senior
Researcher &
Lecturer

Dr. Swantje Westpfahl

Senior
Researcher &
Lecturer

Dr. Pascal Moriggl

Senior
Researcher &
Lecturer

Frank Grimberg

Senior
Researcher &
Lecturer

Dr. Felix Härer

Senior Researcher &
Lecturer

Ilya Misyura

Researcher &
Lecturer

Jona Karg

Researcher &
Lecturer

Hermann Grieder

Researcher &
Lecturer

Franka Ebai

Researcher &
Lecturer

Janine Jäger

Researcher &
Lecturer

Sherdel Käppler

Researcher

Our Understanding of Digital Trust

“Digital Trust means keeping our digital world safe and honest. This means ensuring secure online interactions by protecting data (cybersecurity), respecting privacy (data privacy), safely using new tech (emerging technologies), acting responsibly (ethics and governance), managing risks, and following rules (compliance and audit).”

– Competence Center Digital Trust

Touch the Areas of Digital Trust

Cybersecurity & Resilience
the art of protecting networks, devices and digital data from unauthorised access or criminal use and achieving resilience.

Data Protection
the strive towards protecting (personal) data from improper processing and securing the right to informational self-determination.

Emerging Technologies
those that will have an impact on cyber security or data protection - such as Blockchain, AI, or Quantum Computers.

Digital Responsibility & Ethics
ensures that digital trust is grounded not only in ethical principles but also in accountable and demonstrable practices of responsible action.

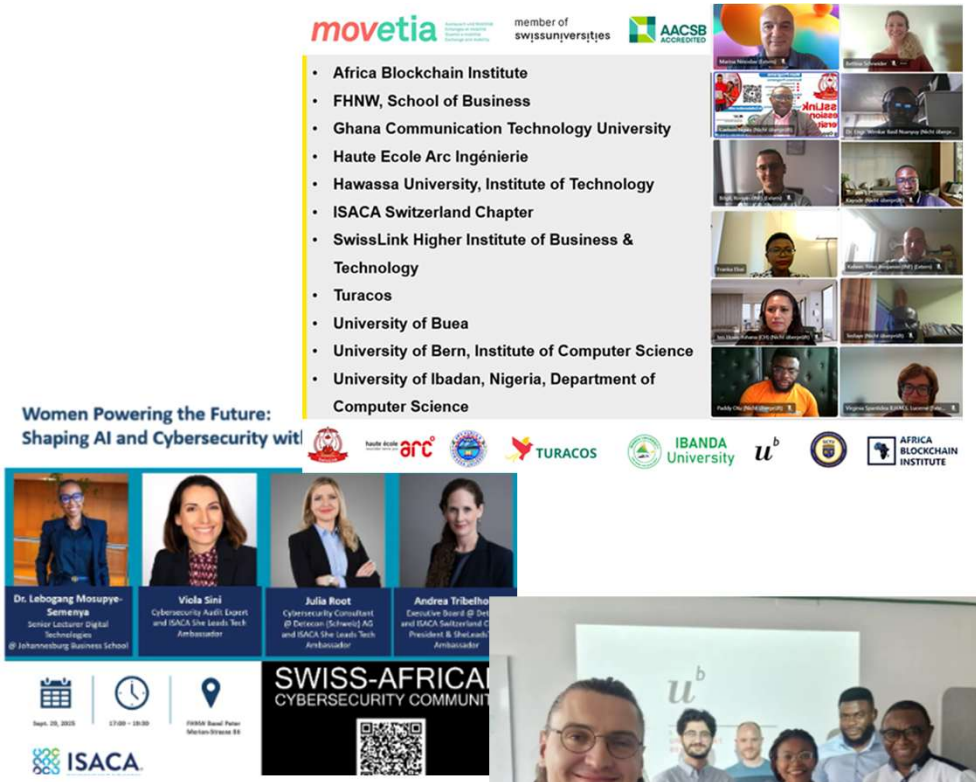
Governance, Risk & Compliance
as a constitutive element of an organisation's value creation – by means of continuous overall consideration of all processes and responsibilities to manage risks effectively and efficiently.

Be Part of the Community

https://www.swissafricacysec.ch

Welcome to the Swiss-Africa Cybersecurity Community

Strengthening cybersecurity through cross-border collaboration, innovation, and research.



The **Swiss-Africa Cybersecurity Community** is a dynamic initiative bringing together universities, researchers, and professionals from **Switzerland and Africa** to address global cybersecurity challenges. Through joint research, knowledge-sharing, and capacity-building efforts, we are creating a sustainable network that fosters **digital trust, resilience, and innovation**.

Following partners support this course:
SwissLinkUniversity, University of Bern and Africa Blockchain Institute


Apr – Jun 2026
Education
Open Lecture on Quantum Technology
JBS & FHNW | Apr - May, 26
Joint Course on Social Engineering
SwissLink & FHNW | Apr - Jun, 26
Collaboration on Cyber Resilience Act (CRA) w/ Student Research
HES-SO & FHNW | May, 26
Joint Teaching on Cybersecurity & Cryptography
Uni Namibia, ACEBR, ABI, FHNW & Uni Bern | May 20 - Jun, 26
Jun 2026
Conference Paper Presentation
Paper Presentation – Society 5.0 Conference in South Africa
Swiss-Africa Cybersecurity Community | Jun 26, 26
Jul 2026
Conference & Workshop
Conference Participation & Community Dissemination
Turacos – Cameroon | Jul, 26
Talk on Software Quantum Threats
University of Bern (TBC) | Jul, 26
Aug 2026
Forum
Swiss Digital Leadership Forum
Swiss-Africa Cybersecurity Community | Aug 31, 26
Oct 2026
Conference
ISACA Europe Conference in Munich, Germany
Swiss-Africa Cybersecurity Community | Oct, 7 - 9, 26
ISACA Emerging Technology Conference
Swiss-Africa Cybersecurity Community | Oct, 26, 26
Nov 2026
General Assembly
General Assembly
Swiss-Africa Cybersecurity Community | Nov, 26
2027
Workshop
Cybersecurity for Entrepreneurial Success
Turacos | Jan/Feb 27

Digital Trust Framework

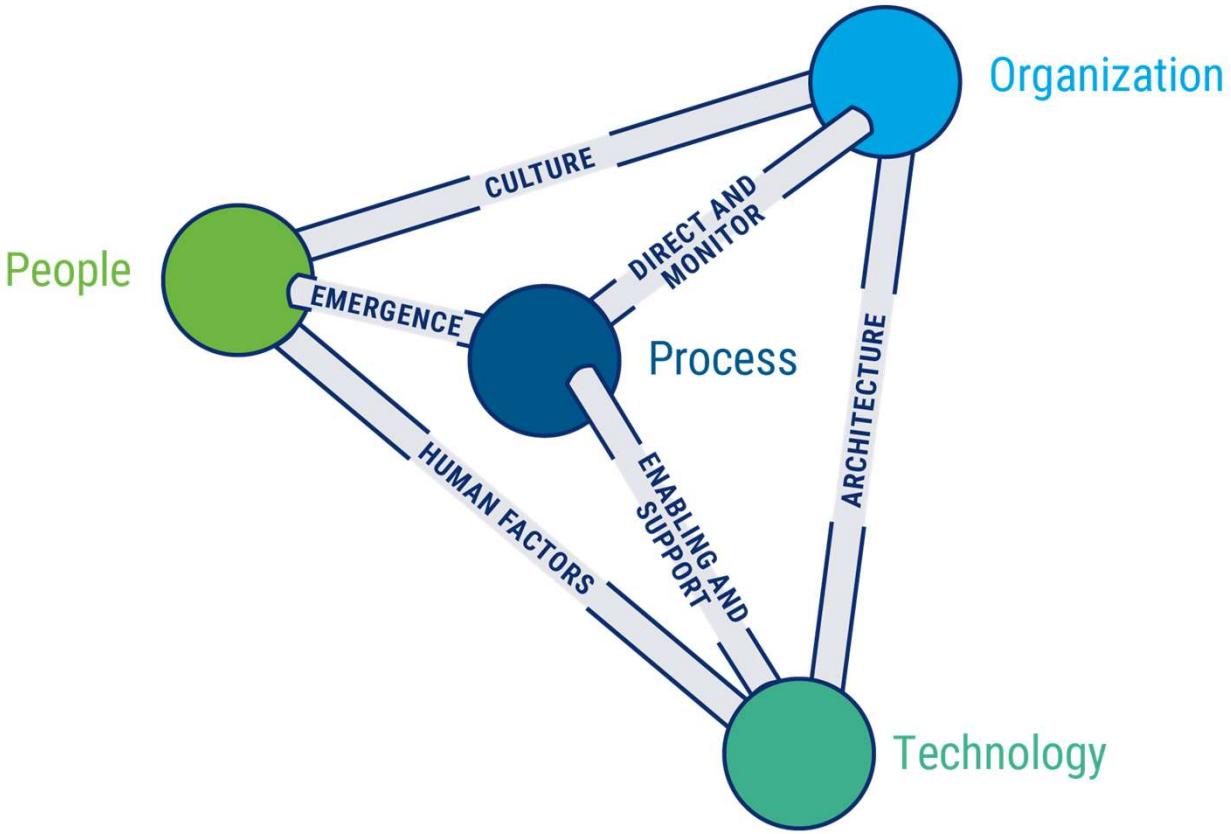
What is Digital Trust?

The **confidence in the integrity of the relationships, interactions and transactions** among providers and consumers within the digital ecosystem.

This includes the ability of people, organizations, processes, information and technology to **create and maintain a trustworthy digital world**.

Digital trust extends beyond cybersecurity and includes privacy, ethics, governance, transparency, resilience, and accountability.

Trust in digital systems replaces traditional face-to-face trust relationships in modern digital societies.



Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 4–5.

Why Does Digital Trust Matter?

- Digital trust improves customer loyalty, reputation, and competitive advantage.
- Consumers increasingly base purchasing and usage decisions on trustworthiness.
- Large amounts of personal data are generated daily, requiring ethical and secure handling.
- Loss of digital trust can lead to reputational damage, financial losses, and reduced adoption of digital services.

Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 4, 6.

FIGURE 2: Digital Trust-related Benefits

Respondents report that high levels of digital trust can lead to the following benefits:

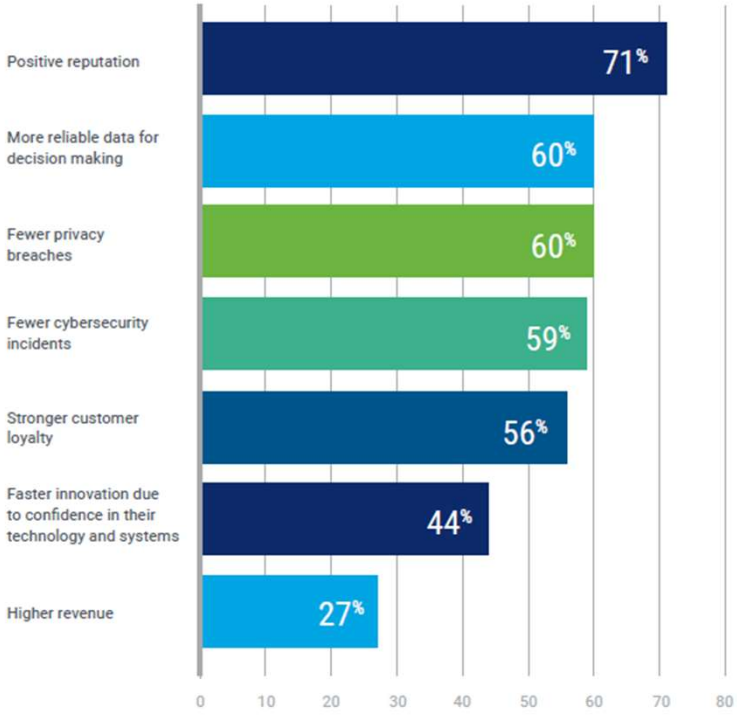
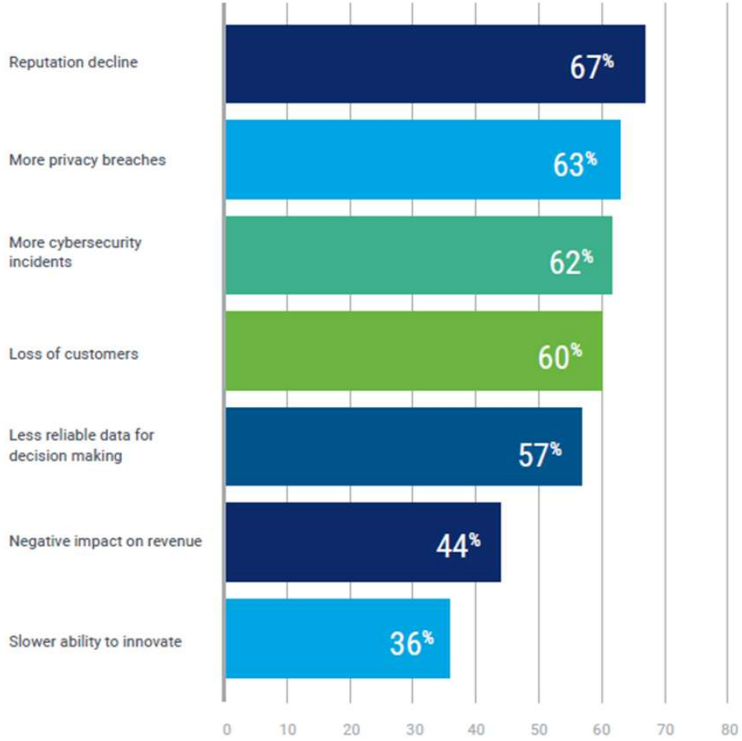


FIGURE 3: Consequences of a Lack of Digital Trust

Respondents say organizations with a low level of digital trust often experience the following consequences:



Source: ISACA 2024 State of Digital Trust Report (read the report): https://www.isaca.org/resources/reports/state-of-digital-trust-2024

Core Dimensions of Digital Trust

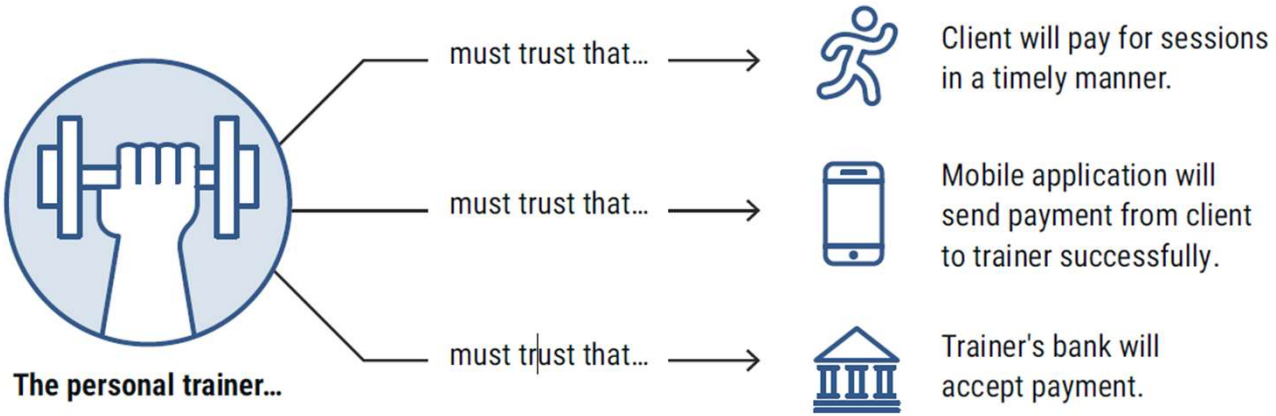
- Quality – reliable and expected service quality.
- Availability – systems and information must remain accessible and accurate.
- Security & Privacy – protection of data and systems throughout the lifecycle.
- Ethics & Integrity – acting according to consumer expectations and values.
- Transparency & Honesty – clear communication about data use and incidents.
- Stability & Resilience – ability to adapt while maintaining reliable services.

Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 4–5.

Digital Trust Across the Ecosystem

- Digital trust must extend across suppliers, vendors, and third parties.
- One weak or untrustworthy participant can compromise the entire ecosystem.
- Organizations must ensure secure processes, patch management, and supply-chain resilience.
- Digital trust is not a one-time activity but a continuous and iterative process.

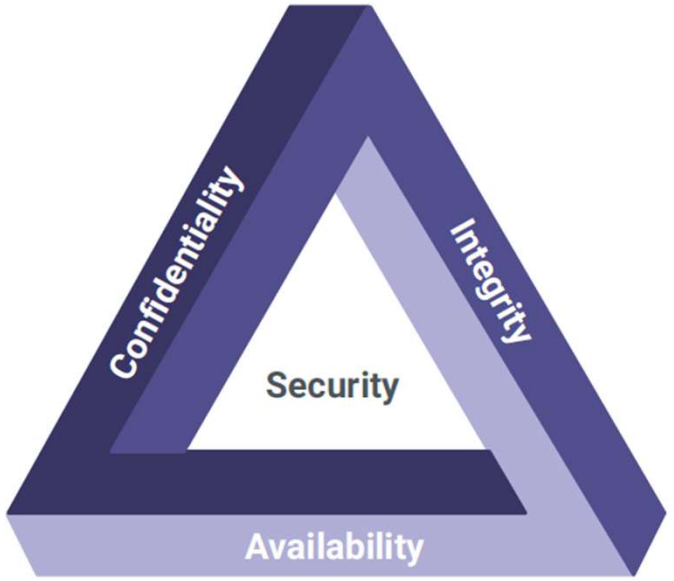
FIGURE 1: Example Digital Trust Ecosystem



Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 5, 8–9,

Digital Trust and Cybersecurity

- Cybersecurity is foundational for digital trust.
- Consumers expect confidentiality, integrity, and availability (CIA) of information.
- Weak security controls, breaches, or outages directly reduce trust.
- Digital trust requires proactive governance, risk management, auditing, and incident response.



Source: ISACA, *Cybersecurity Fundamentals Study Guide, 3rd Edition*, USA, 2021, figure 1.11, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KohiEAC

Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 9–11.

What is Digital Trust?

ISACA has designed a Digital Trust Ecosystem Framework (DTEF) to work in conjunction with existing frameworks to avoid framework overload.

isaca.org/digital-trust

Source: ISACA (2022), Digital Trust: A Modern-Day Imperative, pp. 4–5.

Introduction to Cybersecurity

Discussion

What is Cybersecurity? What do you know about it?

Do you have personal or professional experiences with cybersecurity attacks?

Cybersecurity and Cybersecurity Threats

According to the European Union (EU REGULATION 2019/881):

“Cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"

A threat to cybersecurity means **a threat to network and information systems, its users, and potentially other persons**. Not everyone has the same understanding of cybersecurity (or even the same spelling), but the relation to digital information and infrastructure and its users is always present.

What is the difference between **Cybersecurity** and **IT Security**?

Origin	Document	Spelling	Organization	Type	CIA	Meaning	Motivation	Threat
ISO/IEC JTC1/SC27	27032	Cybersecurity	SDO	V	YES	Only assets intended for the Internet	No differentiation between malicious or unintentional	Only virtual assets connected to the Internet, no physical assets
ISO/IEC JTC1/SC27	27000	Information security	SDO	O[8]	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
ITU-T	X.1205	cybersecurity	Inter-gov	???	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
NIST	SP 800-39	cybersecurity	SDO	V	NO	Risk originating in the Cyber Space ONLY	Only covers malicious origins (cyber attacks)	Only virtual assets connected to the Internet, no physical assets
NATO	National Cyber Security Framework Manual	--	Military	V	NO	Any Risk origination in the Cyber Space (Cyber Threat)	Only covers malicious origins (cyber Threats)	Any asset
Committee on National Security Systems	CNSSI No. 4009	Cyber security	Govt	O	YES	Any Risk	No differentiation between malicious or unintentional	Any asset

European Network and Information Security Agency. (2015). *Definition of cybersecurity: Gaps and overlaps in standardization*. Publications Office. https:||data.europa.eu/doi/10.2824/40690

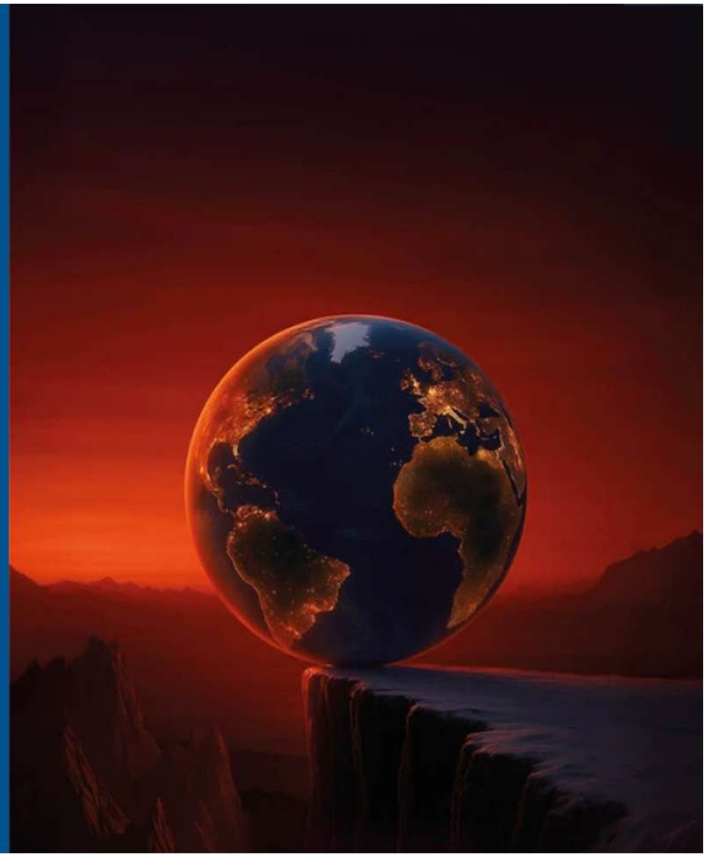
WEF Global Risk Report

Published: 14 January 2026

Global Risks Report 2026

Download PDF

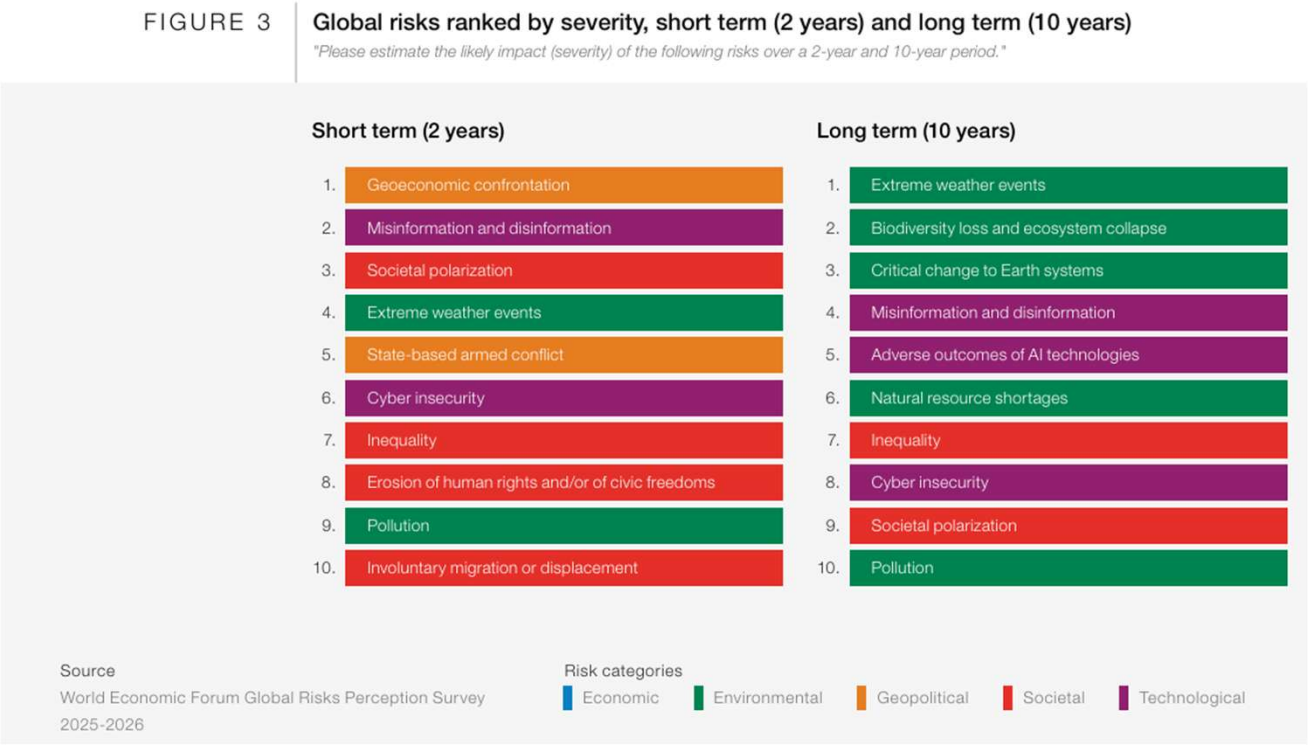
The *Global Risks Report 2026*, the 21st edition of this annual report, marks the second half of a turbulent decade. The report analyses global risks through three timeframes to support decision-makers in balancing current crises and longer-term priorities. Chapter 1 presents the findings of this year's **Global Risks Perception Survey (GRPS)**, which captures insights from over 1,300 experts worldwide. It explores risks in the current or immediate term (in 2026), the short-to-medium term (to 2028) and in the long term (to 2036). Chapter 2 explores the range of implications of these risks and their interconnections, through six in-depth analyses of selected themes. Below are the key findings of the report, in which we compare the risk outlooks across the three-time horizons.



https://www.weforum.org/publications/global-risks-report-2026/digest

WEF Global Risk Report

Technological risks overall remain an ongoing and significant concern for respondents, with Cyber insecurity at #6 reflecting the increasing frequency and sophistication of cyberattacks targeting critical infrastructure, businesses and government.



https://www.weforum.org/publications/global-risks-report-2026/digest

ENISA Threat Landscape

The ENISA Threat Landscape is an annual report,

"*on the status of the cybersecurity threat landscape that identifies prime threats, major trends observed with respect to threats, threat actors and attack techniques and describes relevant mitigation measures*" (ENISA 2023)

PUBLICATION DATE: OCTOBER 1, 2025

Through a more threat-centric approach and further contextual analysis, this latest edition of the ENISA Threat Landscape analyses 4875 incidents over a period spanning from 1 July 2024 to 30 June 2025. At its core, this report provides an overview of the most prominent cybersecurity threats and trends the EU faces in the current cyber threat ecosystem.

Overview of Cybersecurity Threats

Ransomware: Attackers break in and encrypt data, then demand payment for release of decryption keys.

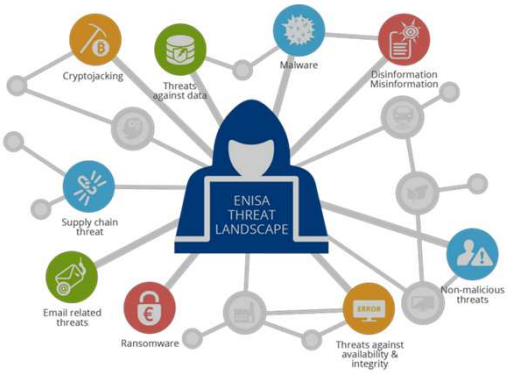
Malware: Malicious programs that will run to have an adverse impact on the victim's system.

Cryptojacking: Secretly using a hacked device for profitable computation (mining Cryptocurrency).

E-mail-related threats: Bundle of threats targeting the human psyche and habits instead of technology.

Threats against data: A data breach or leak is the release of sensitive, confidential, or protected data to an untrusted environment

Threats against availability and integrity: Obstruction of access to victims' data and malicious modification of web data.



TOP 1 TARGET → THE HUMAN
This is why the concept of SOCIAL ENGINEERING is highly relevant

Malware Types 1/3

Viruses	A computer virus is a program or piece of code designed to damage computers by corrupting system files, wasting resources, destroying data or otherwise being a nuisance. Viruses are unique from other forms of malware in that they are self-replicating — capable of copying themselves across files or other computers without a user's consent (Kaspersky, 2022). Need human interaction to start executing.
Trojans	A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of a computer. A Trojan acts like a legitimate application or file to trick the user into loading and executing the malware onto the device. Once installed, it can perform the action it was designed for. A Trojan is not a virus, as it does not replicate itself. (Norton, 2022)
Ransomware	Ransomware is a type of malware that encrypts a victim's files and subsequently demands payment in return for the key that can decrypt said files. When ransomware is first installed on a victim's machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more. Personal files, such as photos and home movies, may hold sentimental value to the victim (Cyber Threat Security Alliance, 2015).
Crypto Malware	Subtype of ransomware that uses advanced encryption methods so files cannot be decrypted without unique key (Kaspersky, 2022). Ransom payment is primarily done through cryptocurrency.

Malware Types 2/3

Adware	There are different types of adware. Some are free ad-supported software which makes ads show up in pop-up windows or on a toolbar in your operating system or browser. At its worst, adware is malware that can gather your personal information by tracking the websites you visit or recording your keystrokes. This aspect of adware is very similar to spyware, which is malicious spying software. Adware resides on your system and displays ads from the inside (Avast, 2022).
Spyware	Software that gathers information about use of a computer, usually without the knowledge of the owner of the computer and relays the information across the Internet to a third-party location (Stern R.H., 2005). It captures everything from keystrokes to the URLs of visited websites (Daniel Jonasson, Johan Sigholm, n.d.). Exploit vulnerabilities to enter the system, no need for human interaction.
Worm	A computer worm is a malicious, self-replicating software program which affects the functions of software and hardware programs. Worms share many characteristics with viruses. But unlike viruses, (1) worms do not need a host file, they exist as separate entities or standalone software; (2) they do not alter files but reside in memory. To spread, worms exploit vulnerabilities or social engineering to trick users to execute them. Once they enter a system, they take advantage of file-transport or information-transport features in the system that allows them to travel unaided (Economic Times).
Keylogger	Subtype of Spyware. Collects data from keystrokes such as usernames, and passwords. Other modern keyloggers can also capture screenshots, emails, browser, chat logs, and more.

Malware Types 3/3

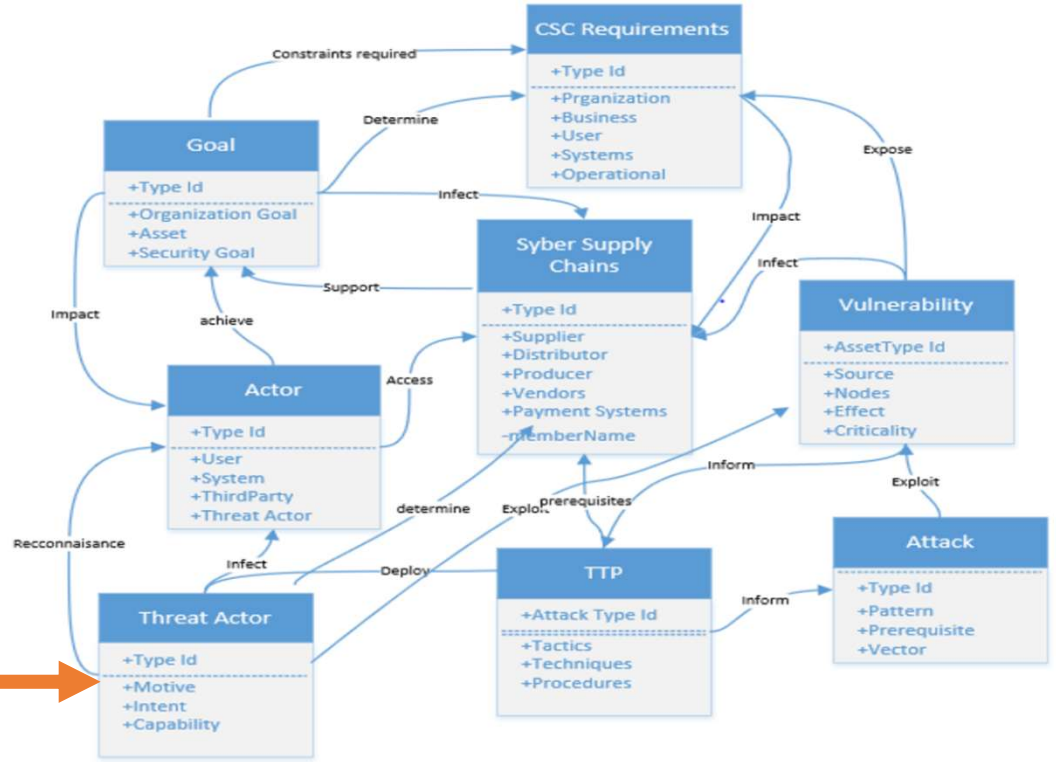
RATs	Subtype of Spyware. **R**emote **A**ccess **T**rojan can conduct covert surveillance by e.g., activating webcams or microphones and CCTV camera. Some variants of RATs are used to create Botnets to carry out DDoS attacks.
Criminal Botnets	Blend of the two words "ro**bot**" and "**net**work." A botnet is a network of computers running bots under the control of a bot herder. Bots are software applications that run automated scripts over a network, while a bot herder is a person controlling and maintaining the botnet. Typical uses include mass email spam, DDoS Attacks, IoT attacks, brute forcing access to Remote Desktop Protocol Servers (malewarebytes, 2022).
Logic Bombs	A logic bomb is a malicious piece of code that is secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs. When this condition is met, the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives. Malwares such as viruses and worms can contain logic bombs as part of their attack strategy. Often inserted by someone with inside knowledge of the system, such as an employee (Avast, 2022).
Backdoors	A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application. Often Rootkits (partially a type of spyware) installed through Trojans are used to create backdoors in systems (Malwarebytes, 2022).

Actors & Attacks

Cyberattack Ontology & Threat Actors

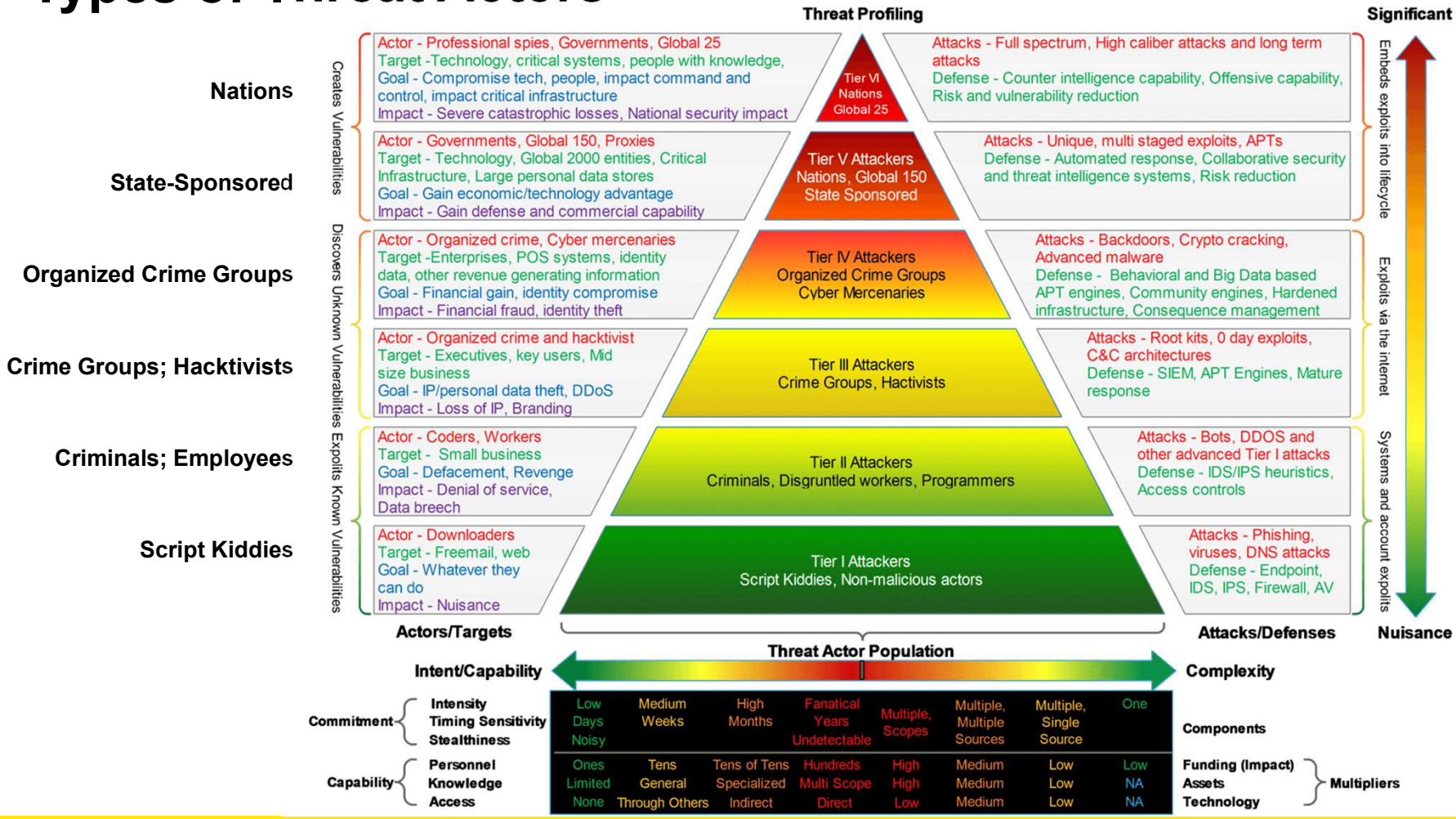
Threat actors deploy Tactics, Techniques, and Procedures (TTP) to **inform** an **attack** to **exploit** a **vulnerability** to either **expose requirements** (business, user, or system data) or **infect** systems to **impact** businesses, users, or systems.

Threat actor: An individual or a group posing a threat. Instigators of risks with the capability to do harm. (NIST, n.d.)

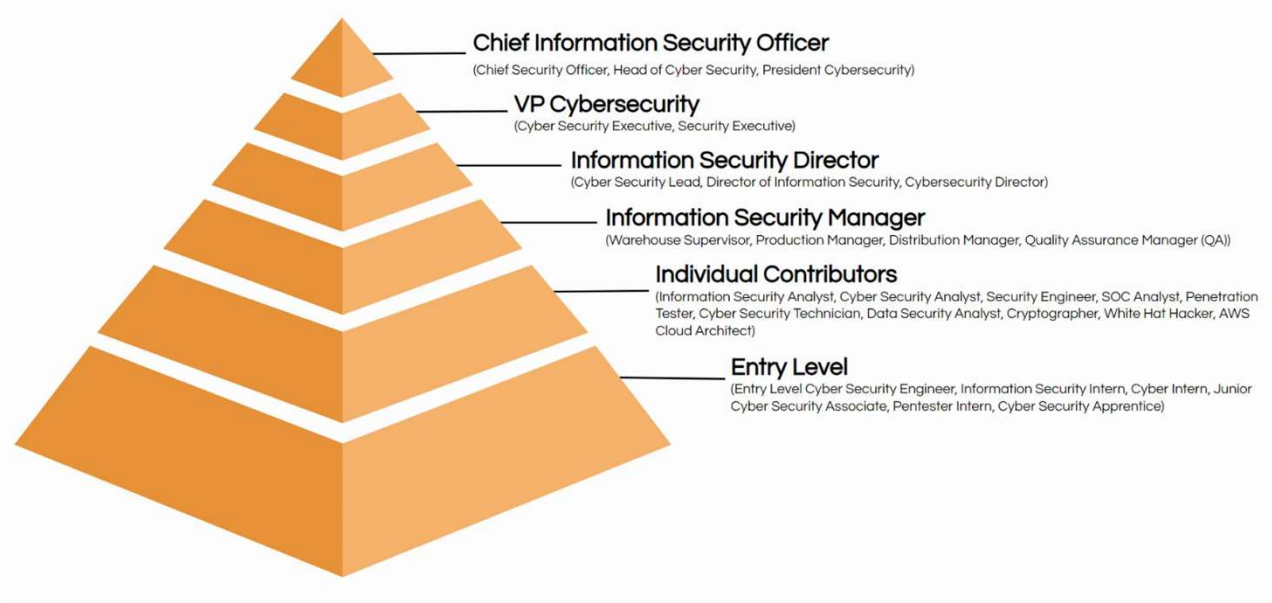


A. Yeboah-Ofori, U. M. Ismail, T. Swidurski and F. Opoku-Boateng, 2021; doi: 10.1109/ICCMA53594.2021.00019

Types of Threat Actors



Cybersecurity Careers



https://blog.ongig.com/job-titles/cyber-security-job-titles/

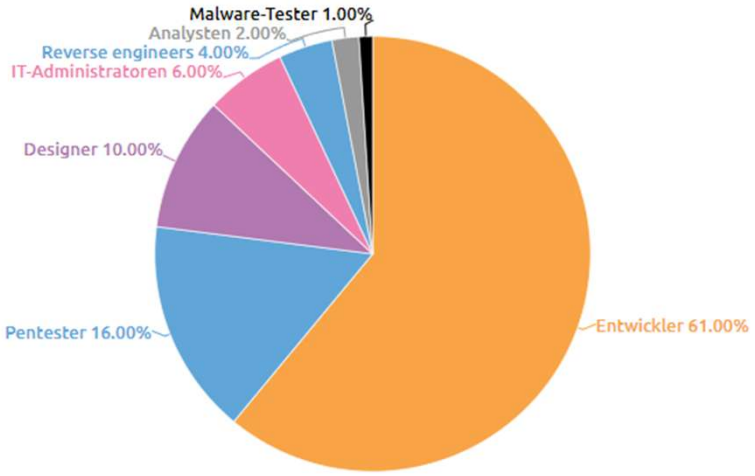
Excerpt: Cyber Security Titles

- Cyber Security Analyst
- Cyber Security Specialist
- Cyber Security Engineer
- Cyber Security Consultant
- Cyber Security Risk Analyst
- Cybersecurity Strategist
- Cyber Security Technician
- Information Security Analyst
- Information Security Architect
- Information Security Manager
- Security Engineer
- Security Researcher
- System Engineer
- SOC Analyst
- Penetration Tester
- Data Security Analyst
- Application Security Engineer
- Information System Security Officer
- Counsel Privacy & Cybersecurity
- Threat Response Analyst

Dark web Careers

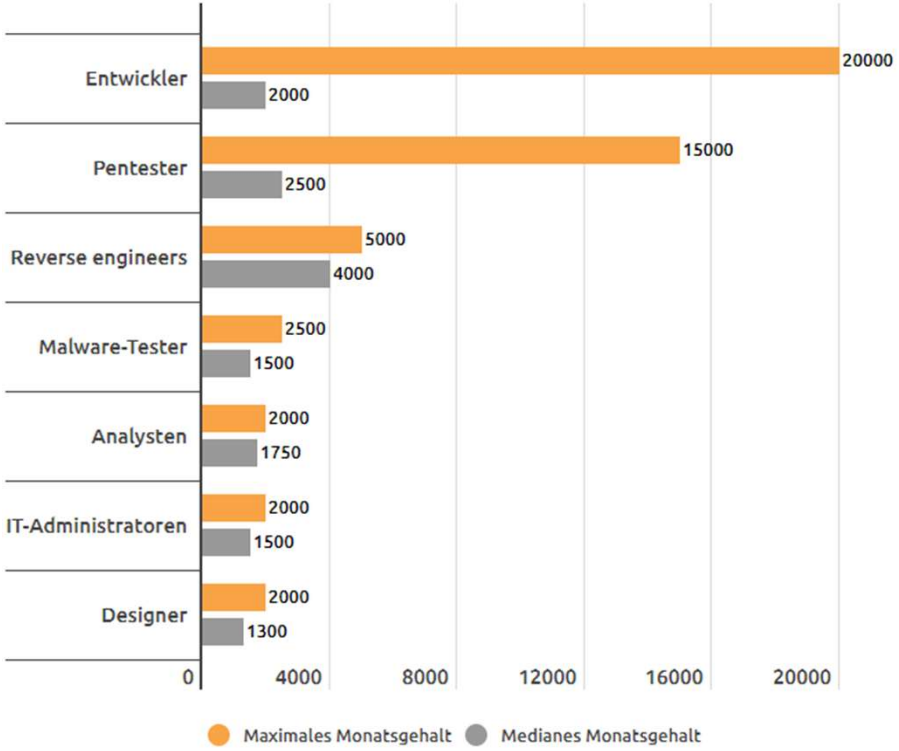
Disclaimer: not encouraged or recommended!

Verteilung der Stellenangebote im Dark Web nach Fachrichtung



Source: Kaspersky , 2023

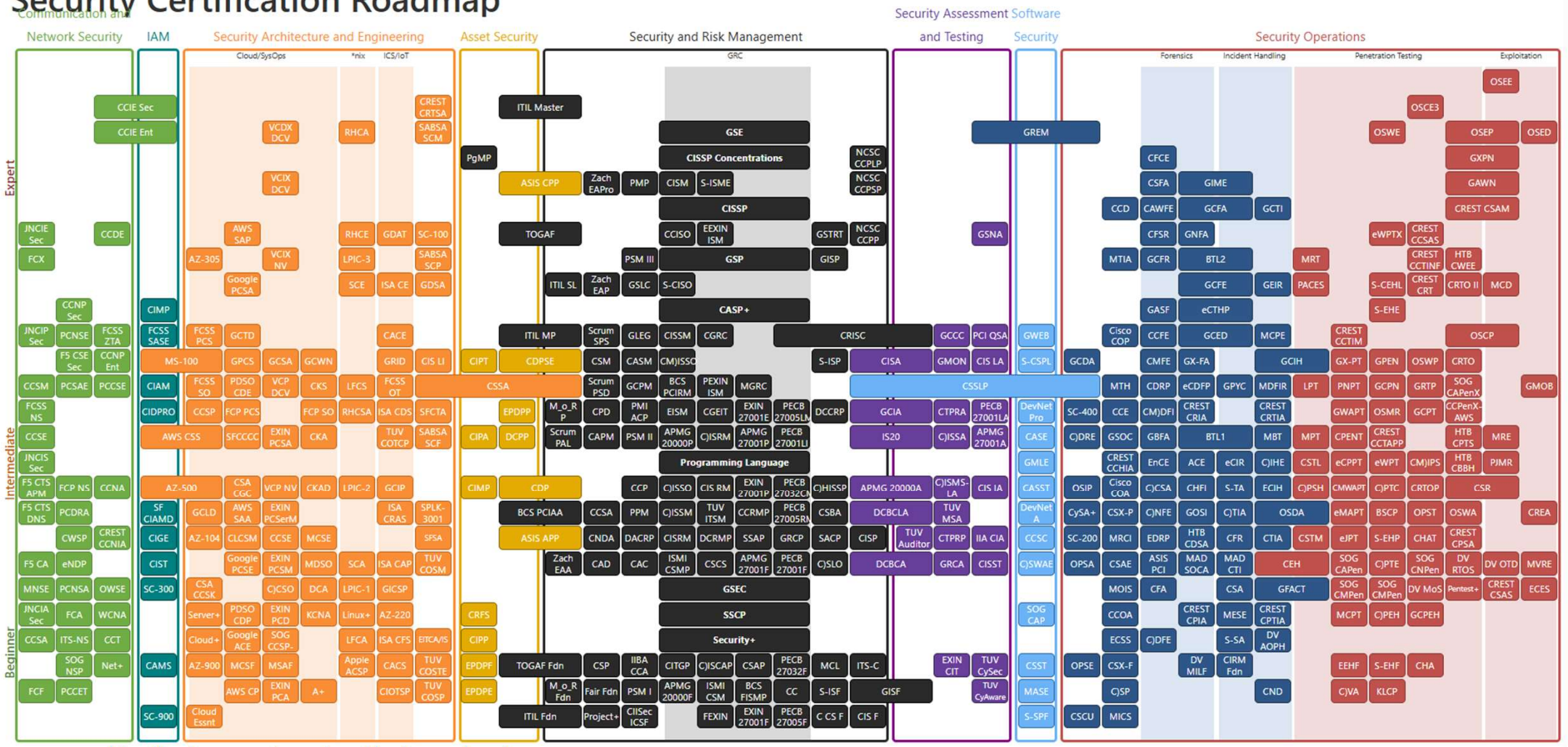
Entlohnung für cyberkriminelle Aktivitäten nach IT-Profilen (in $)



Source: Kaspersky , 2023

https://www.swisscybersecurity.net/cybersecurity/2023-02-10/cyberkriminelle-lieben-diese-it-jobprofile

Security Certification Roadmap



https://pauljerimy.com/security-certification-roadmap/

Course Requirements