Computer risks Schneider Electric

Université Grenoble Alpes
M2 - EECS MISCIT

Team

Mahmoud ABDO
Leader

Liaman ALIEVA
Rapporteur

Armin HASSANZADEH HASSANABAD
Analyst

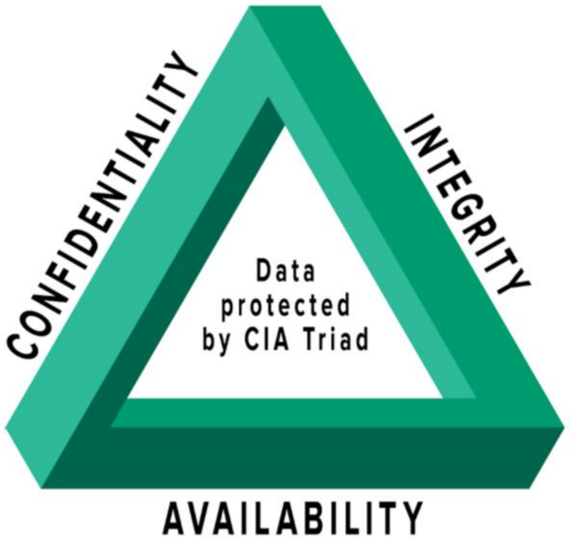
Umair JAVED
Analyst

(1/2) Analysis of computer risks

Confidentiality, Integrity, Availability - is the key pillars of the CIA Triad

DATA BREACH

Unauthorized access to sensitive data (product design, personal data) through security vulnerabilities.



DATA INTEGRITY VIOLATION

Errors or cyberattacks lead to incorrect data in energy or industrial control systems.

SYSTEM DOWNTIME

DDoS attack or system failure leads to service outages for critical infrastructure

(2/2) Analysis of computer risks

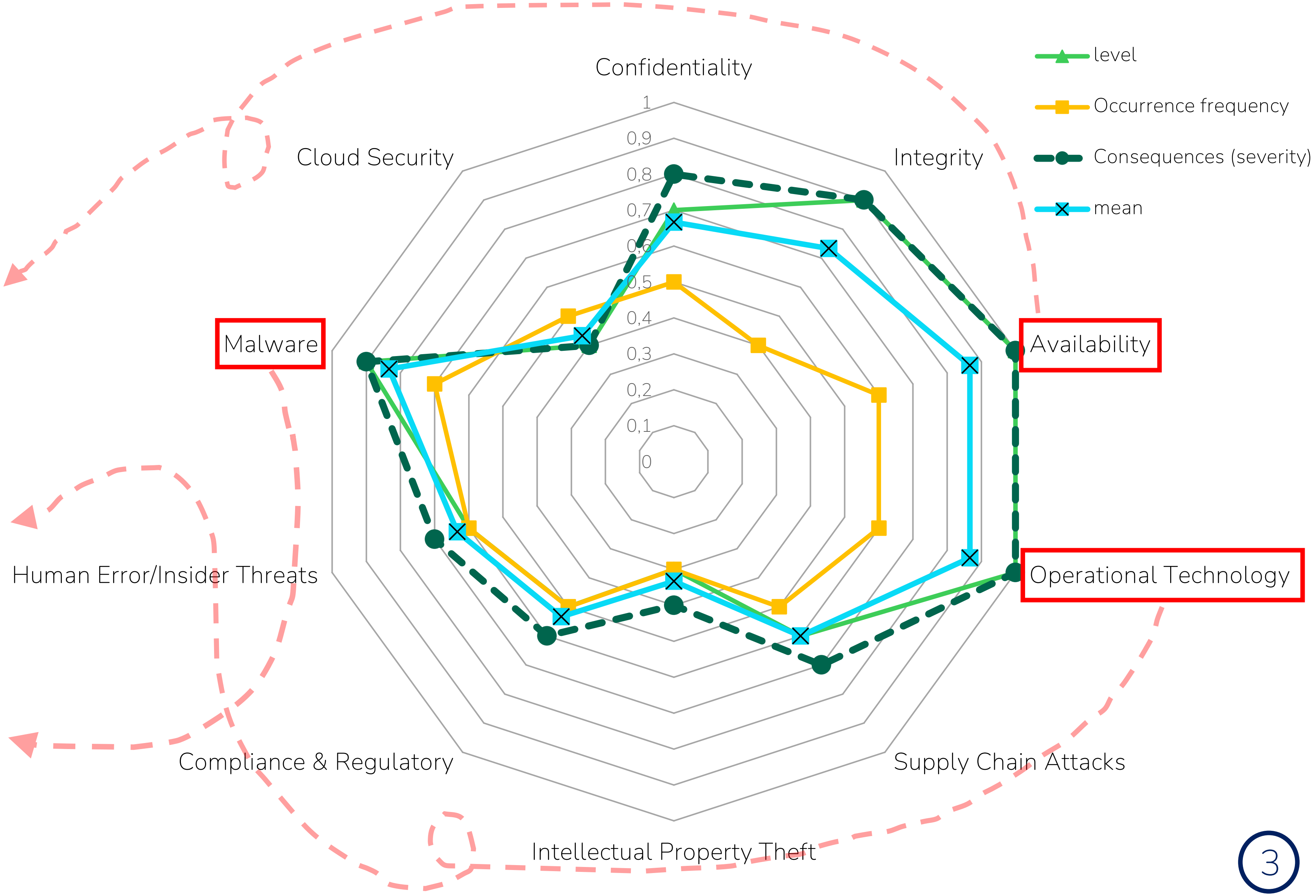
To analyze the Risk level, Occurrence frequency, Consequences the following values were introduced:

🟢 moderate level - less than **0.4**
🟡 significant level - from **0.4 to 0.8**
🔴 critical level - from **0.8 to 1.2**

🔴 **Availability** (0.867) SE supports critical infrastructure. Downtime impacts essential services and safety, so uptime is vital

🔴 **OT security** (0.867) Schneider's industrial control systems are increasingly digitized, making them targets for cyberattacks, which can lead to severe operational damage.

🔴 **Malware** (0.833) Ransomware can halt industrial processes, causing costly downtime and data loss, affecting operations and reputation.



Action plan

Availability

- Implement redundancy
- Disaster recovery plans
- Monitoring systems
- Cloud-based backup
- Regular maintenance

Operational Technology

- Network segmentation
- Patching and updates
- Access Control
- Regular audits
- Intrusion detection systems
- Employee training

Malware

- Anti-malware solutions
- Regular backups
- Email filtering
- Endpoint protection
- Incident Response plan
- User awareness training

Investing now in risk prevention balances future losses

protection today saves costs and reputation tomorrow

Final table

Danger	Dangerous situation	Dangerous event	Risk	consequence	risk estimation		risk evaluation	observations
					Severety (1 to 4)	Proba (1 to 4)	Priorities (1 to 3)	
System Downtime	Failure of critical infrastructure	Hardware failure	Availability	Loss of operational capacity	4 (High)	2 (improbable)	1	Monitoring and update hardware
OT Security Attack	Industrial network breach	Unauthorized system control	destroy the system of the company	production loss	4 (High)	1 (very low)	2	Isolate OT from IT networks, update firmware
Malware Attack	Malware infection through phishing attacks.	employee clicking on the link, not careful	access to customers data	stealing data and damage the company image	2 (Int)	2 (improbable)	3	Deploy anti-malware, train staff, backup systems