SECURING THE FUTURE: THE BA'S ROLE IN CYBERSECURITY AWARENESS

Oleksandr Moskalyuk

BäRN: Hacked! Anforderungen im Zeitalter von Cyber-Threats

August 2024

Oleksandr Moskalyuk

IIBA® – CBAP, CCA

Chief of business process automation department

20+ years of experience

100+ projects

LinkedIn:
https://www.linkedin.com/in/oleksandrmoskalyuk/

Three parts of cybersecurity

- Basic cybersecurity hygiene
- Risk management
- Business Continuity Plan

Basic cybersecurity hygiene
or
authorization, authentication,
and data security.

MFA as
a new normal

Move from Passwords to PassKeys

Principle of less privilege

Re-set default configuration

User roles and logs

Data and information segmentation

Encrypt and backup

Keep software updated

Incidents that could have been mitigated

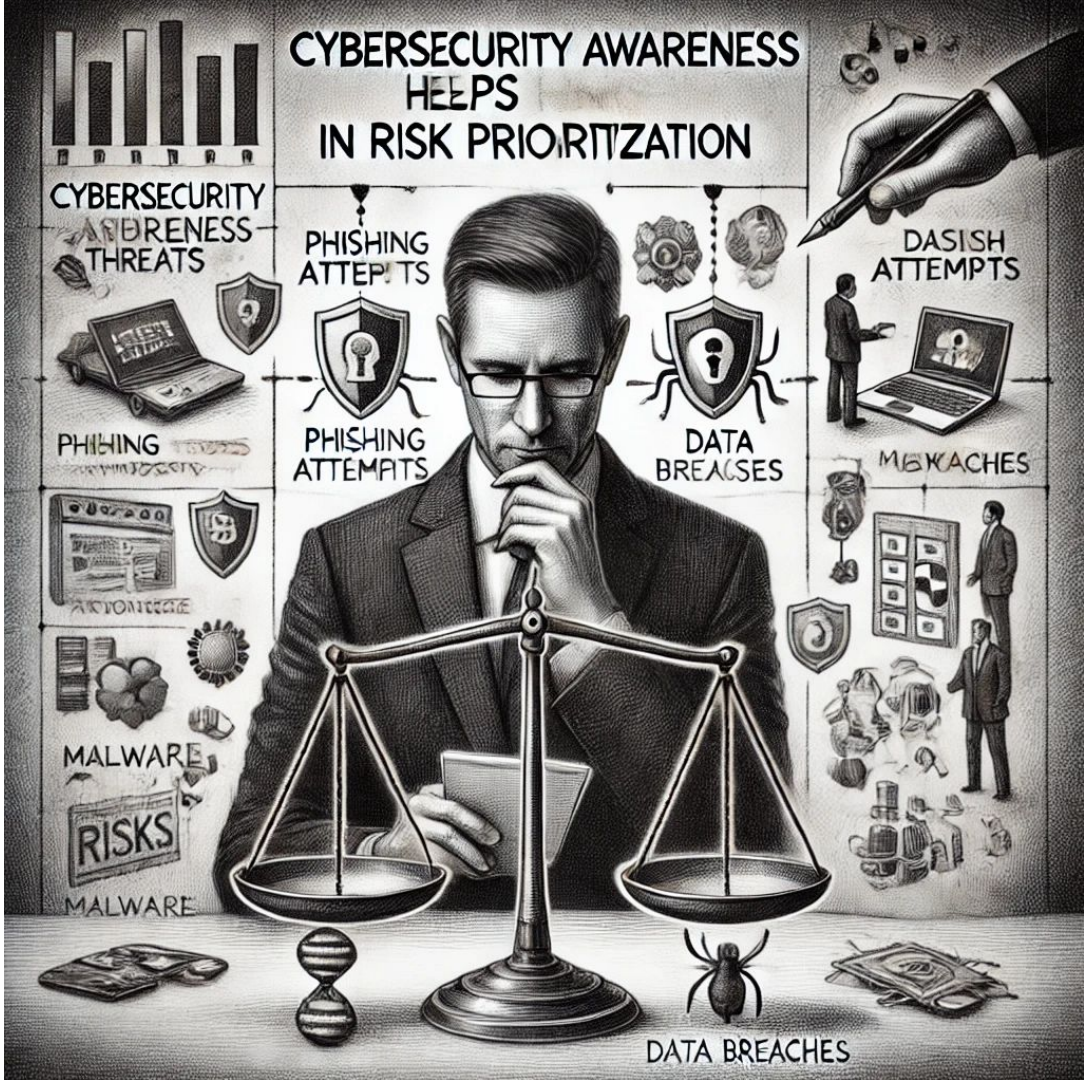
84% Percentage of critical infrastructure incidents where initial access vector could have been mitigated

For a majority of incidents on critical infrastructure that X-Force responded to, the initial access vector could have been mitigated with best practices and security fundamentals, such as asset and patch management, credential hardening and the principle of least privilege.

It is WHEN, not IF

Risk management

Cybersecurity awareness helps in risk prioritization



Several cyber incidents in recent years in Switzerland

1. Data Breach at Swisscom - In autumn 2017, Swisscom, the largest telecom company in Switzerland, reported a massive data breach affecting over 800,000 customers. The breach involved the access of customer data, including names, dates of birth, and telephone numbers, by attackers who gained access rights through a sales partner[1].

2. Cyberattack on Roche - In July 2019, Roche, a Swiss drug and technology company, was targeted by a cyberattack involving malware known as Winnti. The attack was attributed to a hacking group with ties to the Chinese government, although there was no evidence of data theft[1].

3. SITA Data Breach - In March 2021, SITA, a global aviation IT company, reported a security breach where certain passenger data stored on its U.S. servers was accessed by cybercriminals. The breach affected several airlines and travel organizations[1].

4. Ransomware Attack on Comparis - In July 2021, Comparis, a Swiss online consumer outlet, was hit by a ransomware attack, leading to a criminal complaint being filed[1].

5. DDoS Attacks on Swiss Government Websites - Following Ukrainian President Volodymyr Zelensky's visit to Switzerland, the country's federal government websites were targeted by DDoS attacks claimed by the pro-Russian hacker group "NoName". These attacks made several websites temporarily unavailable but did not result in data loss[3][4].

6. Cyberattacks Ahead of Ukraine Peace Summit - Swiss authorities noted an increase in cyberattacks and disinformation campaigns ahead of a Ukraine peace summit in Switzerland. The attacks were suspected to be linked to Russia, given its opposition to the summit[2].

7. Ransomware Attack on Xplain and Federal Railways - In May 2023, a ransomware attack on the IT company Xplain affected the Swiss Federal Railways and various cantonal authorities. The attack, attributed to the Play group, resulted in the theft of operational data and commercial correspondence. Data was encrypted and some was published on the darknet[4].

Citations:

[1] https://www.cyberlands.io/topsecuritybreachesswitzerland
[2] https://therecord.media/ukraine-peace-summit-switzerland-cyberattacks-warning
[3] https://www.swissinfo.ch/eng/politics/switzerland-hit-by-cyberattack-after-ukraine-president-s-visit/49136116
[4] https://www.swissinfo.ch/eng/politics/swiss-government-and-federal-railways-hit-by-cyberattacks/48583086
[5] https://www.euronews.com/business/2023/09/04/half-of-switzerlands-large-companies-have-been-the-victim-of-a-cyber-attack
[6] https://www.connectontech.com/new-obligation-to-report-cyber-incidents/
[7] https://penta.ch/insights/swiss-cybercrime-nearly-doubles-in-six-months
[8] https://unn.ua/en/news/switzerland-announced-an-increase-in-cyber-attacks-and-disinformation-on-the-eve-of-the-peace-summit

Source:

https://www.perplexity.ai/search/what-were-recent-cyberincident-dCxheYqxSl6QyU3WYoDIWQ#0

You can not protect from all possible threats

- CrowdStrike incident (https://en.wikipedia.org/wiki/2024_CrowdStrike_incident)
- Google deleting Australian pension found data (https://www.perplexity.ai/search/what-was-recent-cybersecurity-cvxk7WErQ_WSLNcgyce8OQ#1)
- Kyivstar attack and its affect on other businesses (https://www.perplexity.ai/search/what-was-recent-cybersecurity-cvxk7WErQ_WSLNcgyce8OQ#2)

Priority = Probability * Impact

Threat relevance (or Risk Probability)

Relevance Value	Description of the threat Tactic, Technique, or Procedure (TTP) Relevance to the Organization
Confirmed (5)	It has been seen by the organization.
Expected (4)	It has been seen by the organization's peers or partners.
Anticipated (3)	It has been reported by a trusted source.
Predicted (2)	It has been predicted by a trusted source.
Possible (1)	It has been described by a somewhat credible source.
N/A (0)	The threat event, tactic, technique, or procedure is not currently applicable.

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Impact Assessment Scales (or Risk Impact)

Value	Impact SEVERITY of Threat Events	RANGE of Impacts of Threat Events
Very High (10)	Threat expected to have multiple severe or catastrophic adverse effects.	Effects are sweeping, involving almost all organizational cyber resources.
High (8)	Threat expected to have severe or catastrophic adverse effects.	Effects are extensive, involving most organizational cyber resources, including many critical resources.
Moderate (5)	Threat expected to have a serious adverse effect.	Effects are substantial, involving significant organizational cyber resources, including some critical resources.
Low (2)	Threat expected to have a limited adverse effect.	Effects are limited, involving some organizational cyber resources, but no critical resources.
Very Low (0)	Threat expected to have a negligible adverse effect.	Effects are minimal or negligible, involving few if any organizational cyber resources, and no critical resources.

Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Risk prioritization

Risk	Probability	Impact	Priority
#1 Data Breach	Expected (4)	High (8)	2 (4*8 = 32)
#2 Unauthorized access to the system	Possible (1)	Moderate (5)	5 (1*5 = 5)
#3 Cyberattack using malware	Expected (4)	Very High (10)	1 (4*10 = 40)
#4 DDoS attack	Confirmed (5)	Low (2)	3 (5*2 = 10)
#5 Third party payment gateway malfunction	Possible (1)	High (8)	4 (1*8 = 8)

Talk money to business

$$\text{Return on Investment (ROI)} = \frac{\text{Net Return}}{\text{Cost of Investment}}$$

Return on security investment (ROSI)

ROSI = (Security cost avoided - Cost) / Cost

ROSI = (Annual Loss Expected * Mitigation Rate – Cost) / Cost

ROSI = [($Single Loss Expectancy *Annual Rate of Occurrence) * Mitigation – Cost] / Cost

Single Loss Expectancy = Direct loss from the cyber incident
+ recovery cost
+ lost benefit for the recovery time
+ fines and compensations

Business Continuity Plan

Incident Response, Recovery, and Remediation

1. Incident Response Team (IRT)
2. Recovery Time Objectives (RTOs)
3. Recovery Point Objective (RPO)
4. Test your backups

Let’s summarize:

- Basic cybersecurity hygiene
- Risk management
- Business Continuity Plan

6th EUROPEAN BUSINESS ANALYSIS DAY

www.ba-day.com

15 May 2025

SAVE THE DATE

Special Save the Date ticket
for only 125 EUR
till the end of August

Thank you!

Time for the questions