Simply in good hands

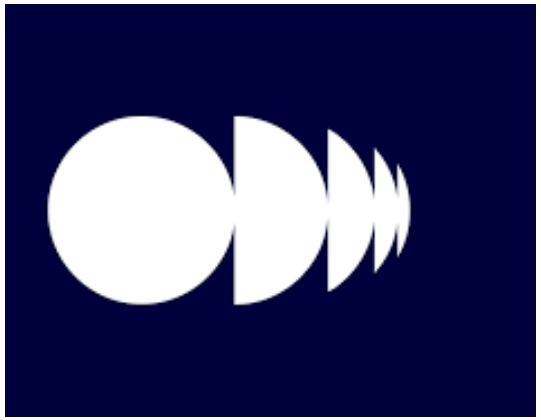
Marcel Zumbühl,
Group CISO Post
Board Member SPCS
Co-President ISSS

15/12/2025

Overview

- **Who we are and why**
- Customer Centricity – Digital Trust
- Resilience – Participatory Security
- Cyber Riskmgmt - Beyond

Swiss Post Group and Cybersecurity



Swiss Post Group and Cybersecurity

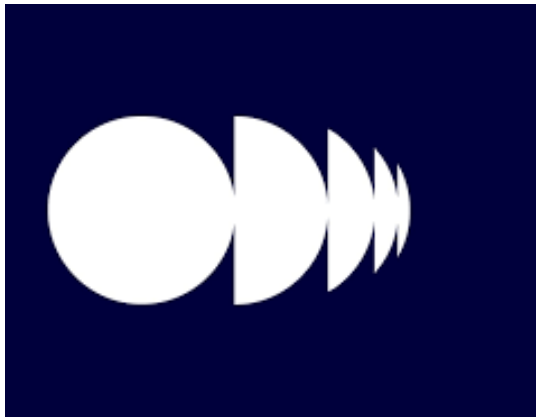
Swiss Post Group – 60’000 employees, 4 markets: Banking, Logistics, Public Transport, Communication Services, 100% stocks held by Swiss Confoederation.

Figures – 7’626MCHF operating turn-over, 324MCHF group profit, 86BCHF assets under mgmt, 183M passengers in Postbus, 76/100 customer satisfaction, 180M parcels

Customer Expectations – Confidence/Trust, Reliability, Speed, Digital Services

Norms and Standards - ISO 27001, ISO 22301, ISO 20000, PCI-DSS, SWIFT, eVoting Certificate, Digital Health Certification

Regulations – Post Regulation, Critical Infrastructure, Swiss Monetary Authority, ISG, Swiss GDPR, Swiss Health Authority



Marcel Zumbühl

Group CISO	Swiss Post
Board of Directors	Swiss Post Cybersecurity AG
Co-President	ISSS Information Security Society
Lecturer HSG, UZH, HSLU, Bocconi	Risk Communication, CISO Module
Lecturer Uni of Rochester/Berrn	Cybersecurity for Boards
Bug Bounty Switzerland	Advisory Board
DigitalSwitzerland	Cyber Security Committee
Credit Suisse	CISO Digital Pivate Banking
	Head Security Controls Steering
Swisscom Schweiz	Chief Security Officer
Accenture	Mgr Communications & Hightech

Uni Rochester-Bern, IMD, London Business School, Uni Bern

Swiss CISO Award Winner

Married, adult son, CH/ITA dual citizen
Languages, sports, saxophone, carpenter

Our Vision - Information Security

Freedom for our customers needs trust.

Trust requires secure solutions in the physical and digital world of tomorrow.

Safety is the DNA of our products.
Today for the future.

"Simply in good hands"

Mission

What do we do and what goals do we pursue

Information Security Post

More than 100 employees in 7 teams – Diversity opens perspectives

Security Management

1400	Employees in I/T
>100	Employees in InfoSecurity
nationalyl/internationaly connected	
7x24h	Cybersecurity Operations Centres
100	Penetration Tests per Year
1	One of Europe's largest BugBounty
ISO	Certified Security

Deferred Attacks per Month

20	Directed Attacks
200	Attackwaves against Customers
8 000	Virus Infection Attempts
13 Mio	Spam/Phishing

Attack Trends

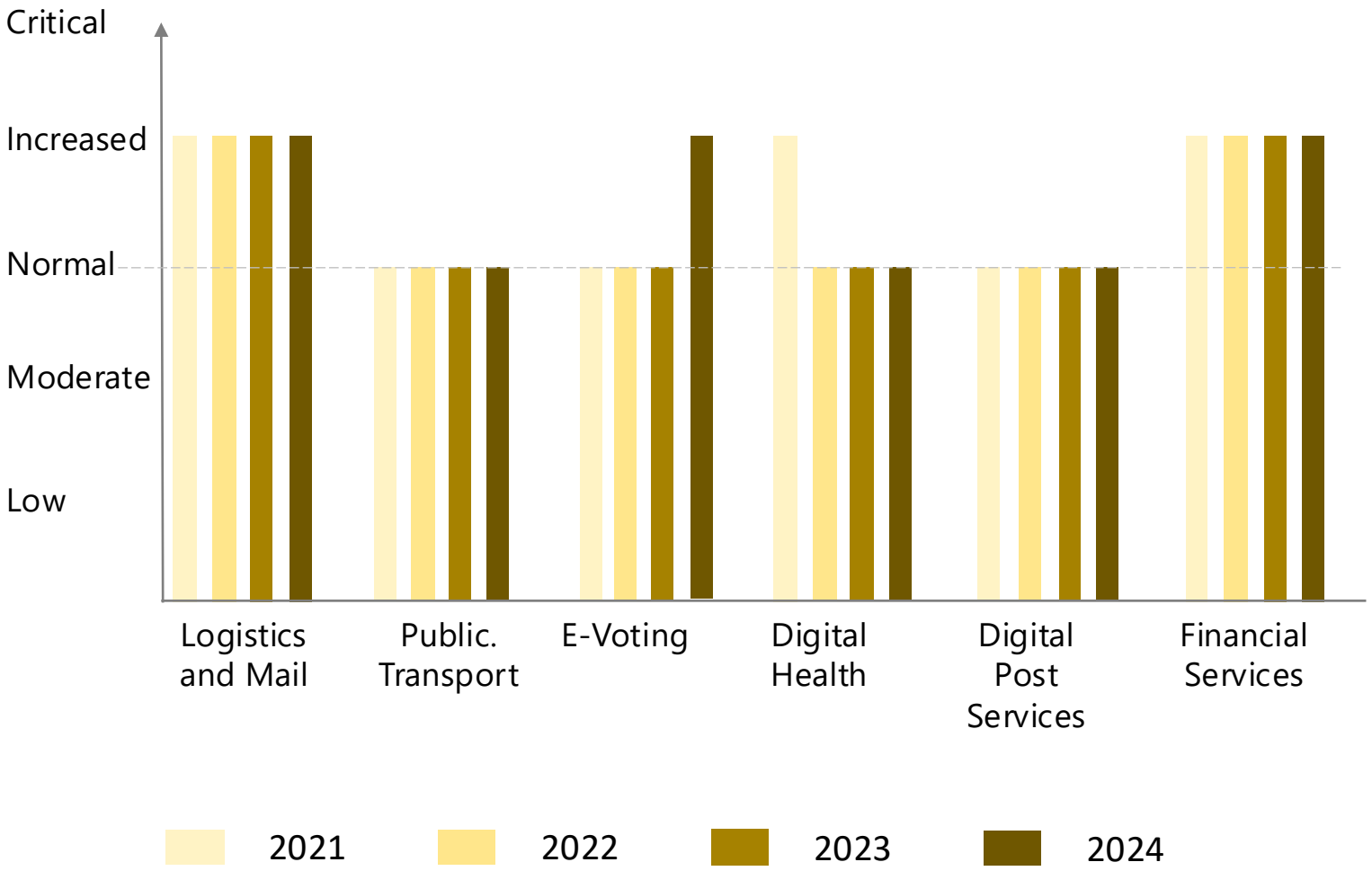
Identity Fraud
Online Fraud
Ransom Attacks

Industries in Target

Finance and Payment
Mail/Logistics
Electronic Voting

Cyber Threat Global View by Market

Attackers worldwide continue to focus on logistics and financial services



Sector	Trend since last report
Logistics and Mail	Attacks on logistics companies and suppliers. New additional focus on maritime logistics
Public transport	Carpools, mobility companies and the automotive industry are the target of data thefts. Acts of sabotage at railway companies EU
E-Voting	Increase in the threat of geopolitical tensions, manipulation/disruption worldwide
Digital Health	Attacks against hospitals, doctors' surgeries and pharmacies remain high. Extortion on impending fines
Digital Post Services	Phishing/spoofing attacks against postal companies remain high
Financial Services	In addition to attacks on financial institutions and credit cards, mobile payment is also incr. being targeted

Information Security Strategy Post

Participatory Security

Spatial Computing

Artificial Intelligence

Operational Tech Security

Machines as Customers

Quantum Computing

Information Security Strategy 2025-2028

Area of Action	**Secure Digital Ecosystems** Increase Security Focus with Partners, Fostering Security Culture	**Trustworthy Identities** Consolidated, simplified and secure Identity Spaces	**New Technologies and Methods** Products and Services at Security State of the Art
Focus 2025	– Embedded Security – Security in Supply Chains – Info Leak Prevention – **Customer Centric FraudMgt**	– Passwordless Self Service – Seamless Collaboration – **Identity First Security** – Mgmt Priviledged Access	– Firewall Management – **Secure AI** – **Zero Trust** – **Quantumproof Cryptography**

* Multiyear Projects

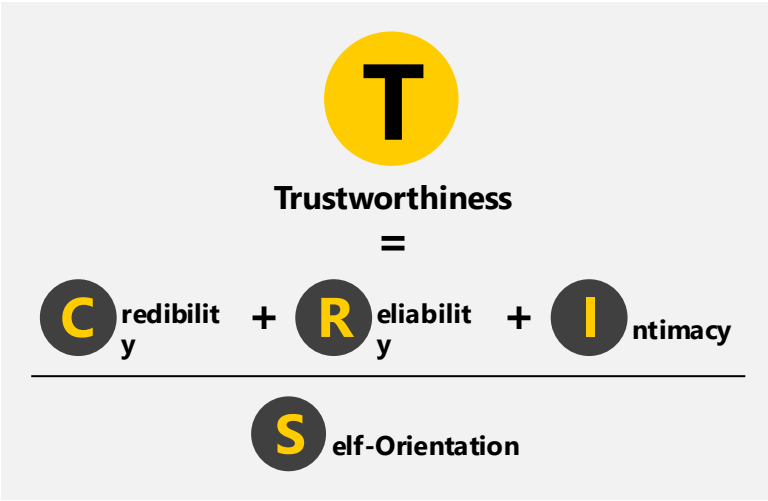
Overview

- Who are we and why
- **Customer Centricity – Digital Trust**
- Resilience – Participatory Security
- Cyber Riskmgmt - Beyond

Challenges of digital trust

Usefulness and perceived personal risk

Trust	Asymmetrical relationship based on perception and experience
Perception is reality	Reasons for trust; who will take care of the case if something goes wrong, and how will I be treated then?
Complexity	Digital systems are very complex and difficult to capture and expand.



Digital trust	Non-experts are supposed to trust systems without being able to look behind the scenes. The perceived personal risk depends on the experience and must correspond to the benefit.
Security is a process	Information security is the key to our customers' success. Safety is based on the interaction between man and machine. Transparent communication helps to weigh up risks and build trust.

Trust in the security of digital products and services

Survey results – Despite efforts the indecisiveness of our customers has increased. Majority positive

2023

Swiss Post is very trustworthy when it comes to the security of digital services.

Agree with the statement
Neutral
Rejection of the statement
Don't know

2025

Swiss Post cares for Information Security and Data Privacy

Case Study – Ticket Control

Cyber incidents can build trust. When communication is prompt and transparent.

Starting situation	Investigative security researcher finds a gap in the portal of the fare dodger database "ticketcontrol.ch" in November 21 and informs Swiss Post on January 22, shortly before a media report on Swiss television – on a Friday evening.
Reaction Information Security	Immediate in-depth analysis of vulnerabilities with the goal of having a whole picture. Information to the Data Protection Authorities. Close the security gap immediately.
Communication	Talk about the whole case via PostBus media spokesperson, not just about the points that Swiss television already knows. Show responsibility and show what we learned from it. The resulting media report was smaller than expected.
Opportunity	Security incidents are opportunities to show that the company acts responsibly and customer-oriented. If they are mastered well, trust and customer loyalty increases.

Case Study - Ransom Attack

Schweizer Post kämpft gegen Cyberangriff in Deutschland

Von Keystone-sda / cwi, 28. April 2025 um 12:03

SECURITY DIE POST CYBERANGRIFF CYBERCRIME BREACH DEUTSCHLAND

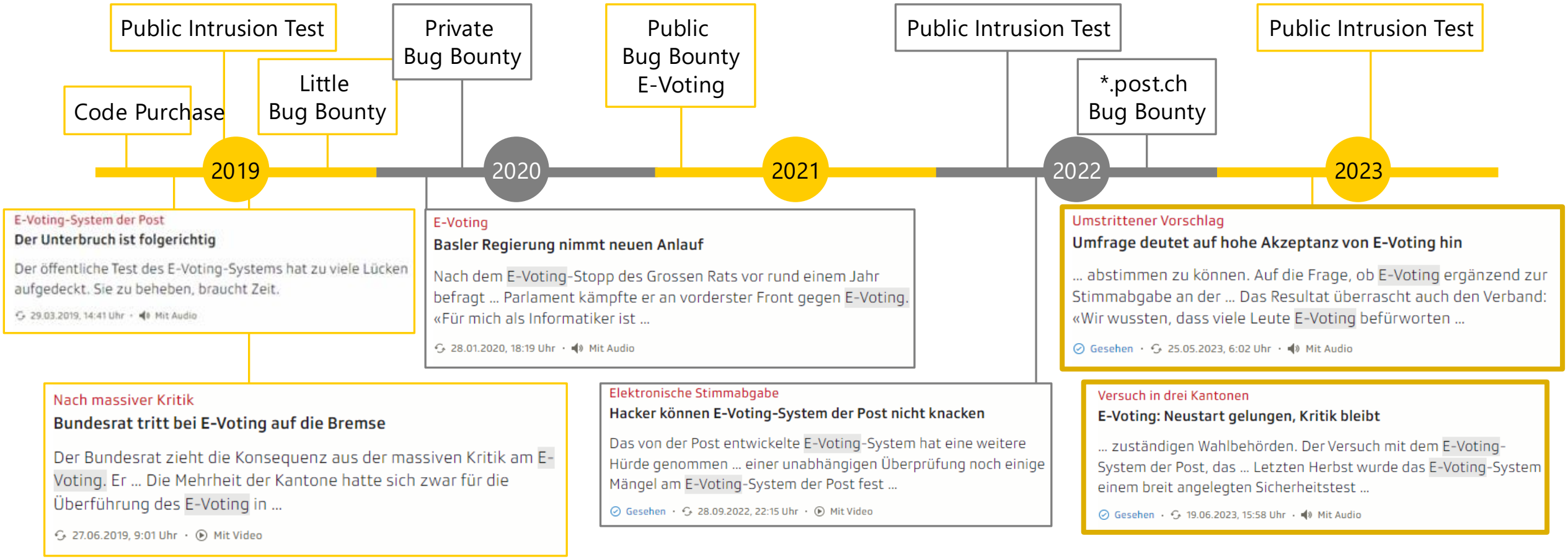
Foto: Die Schweizerische Post

Ein Cyberangriff hat den Betrieb von Swiss Post Cargo Deutschland beeinträchtigt. Dabei sollen auch Kundendaten abgeflossen sein, schreibt die Post

Situation	Criminals provoke IT outage
Reaction	Taskforce. Damage assessment and containment. Establish emergency operations. In depth analysis and rebuild
Proactive Comm	Proactive. Authorities, customers and media. Media coverage was
Benfit	Demonstrate customer focus and responsibility
Learned	Don’t forget employees. Safe copies of financial data. Call in the pros. No blame game. Blame is on attackers

Case Study – Media Echo E-Voting

Participatory security and transparency lead to positive reporting.



What: Headlines – srf.ch

Cyberincidents are not the end of the world
ISSS Courage Award Winner 2025

Underpin customer trust

Be Courageous

Be Proactive

Reach out

Do not become a hostage

Data Sport AG

Overview

- Who we are
- Customer Centricity – Digital Trust
- **Resilience – Participatory Security**
  > People are the strongest link
  > Bug Bounty Programme
  > Security Collaboration with suppliers
  > Security Champions Programme
- Cyber Riskmgmt - Beyond

People are the Strongest Link

Thanks to courageous employees we detected and stopped a ransome attack

Attacks – Most attacks target eiter employees at the periphery of the organisation or top mgmt.

Weak Signals – Attacks are camouflaged and not easily detectable. Watch-out for things that just don’t look right.

Speak-Up Culture – Encouraging employees to speak-up allows for early detection of weak signals.

Bug Bounty in a nutshell

Security is a continuous process that Swiss Post takes very seriously as a progressive company.

That's why we work with a global community of ethical hackers to continuously improve our information security.

Interested hunters can apply to participate in the private bug bounty program here:

- **post.ch/bug-bounty**
- **bugbounty@post.ch**

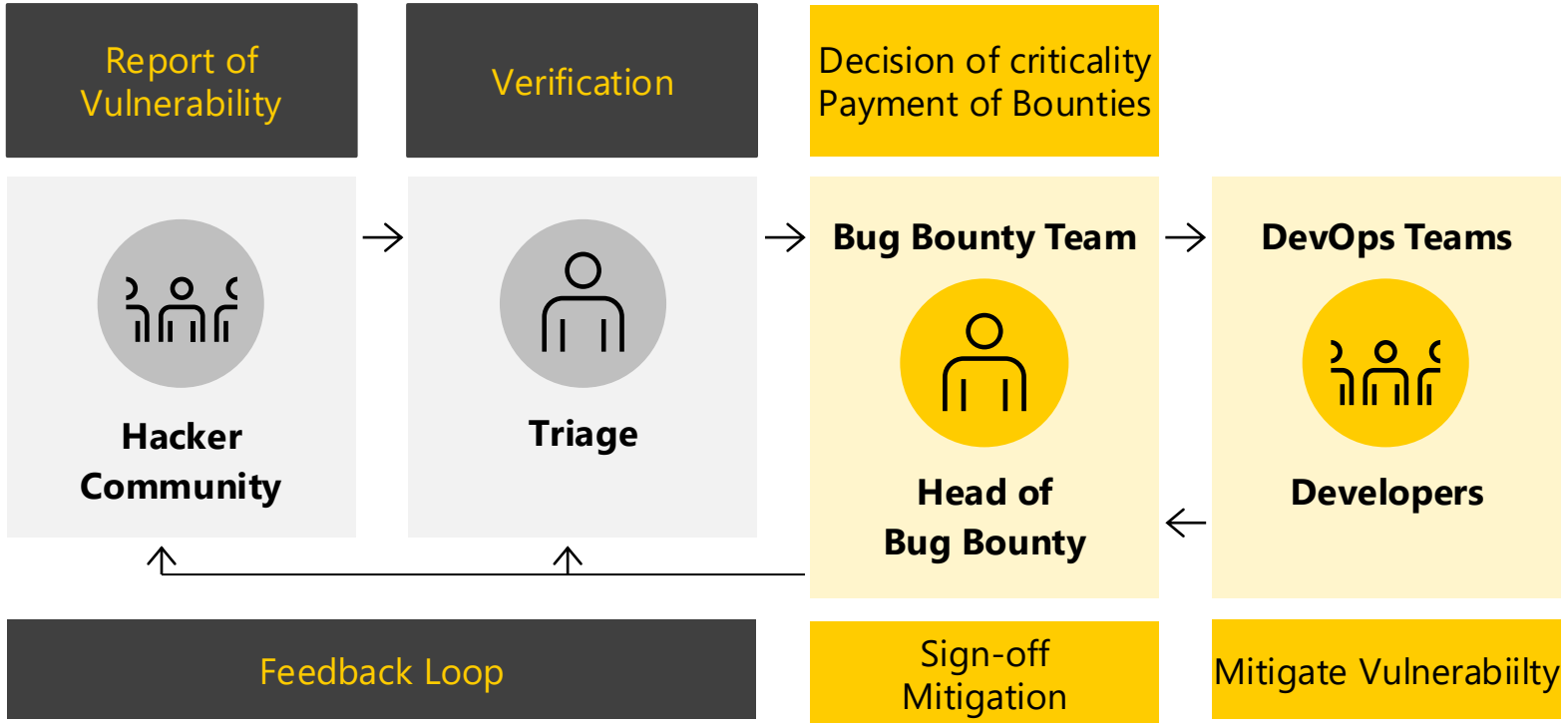
Finding vulnerabilities
(Bugs)

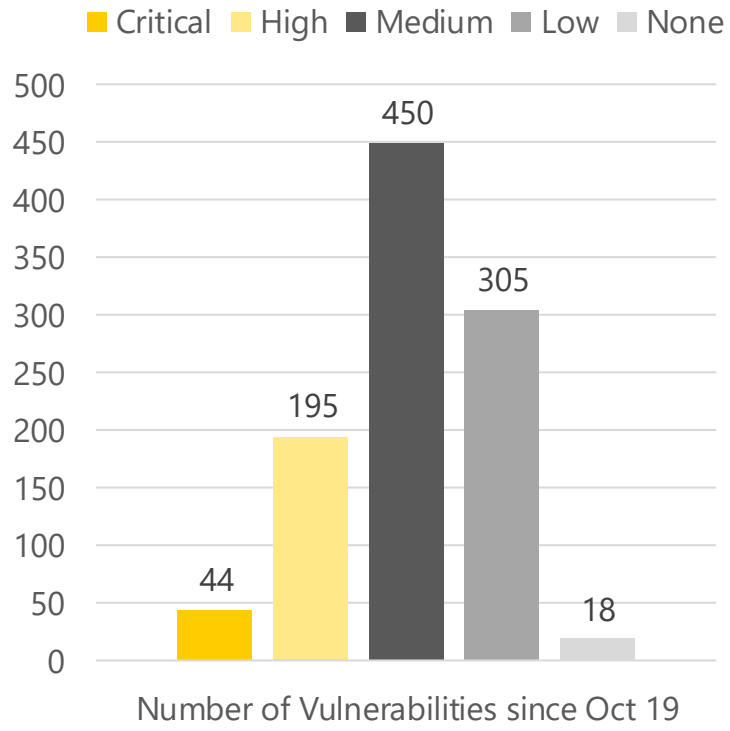
by ethical hackers
(Hunter)

for a reward.
(Bounty)

Bug Bounty Post

Swiss Post is pioneering Bug Bounty in Europe in collaboration with ethical hackers.
Post uses the crowd know-how to increase security of all services





Step-by-step improvement of the security maturity

Systematic development of bug bounty programs

Privates Bug Bounty

Goal - Continuous Testing
& Security Transformation

Duration depends on maturity

Bounties max. 5k CHF

Hunters ca. 50

Security Challenger

✓ Maturity check passed
✓ Bugs fixed
✓ Transition to public prog

Security Excellence

✓ Public Exposure
✓ Continuous Improvement

Public Bug Bounty

Goal - Full Insight
& Digital Trust Gain

Duration continuous

Bounties max. 10k CHF

Hunters > 1000

Security Champion Community

Developing security with committed people

Contact person – For security-related challenges and questions

Motivator – High security maturity in projects

Promotors – Security is an integral part

Coach – Know-how sharing, security awareness

Technician – Vulnerability Assessment, Threat Modeling, Choice of Analysis Tools, Best Practice

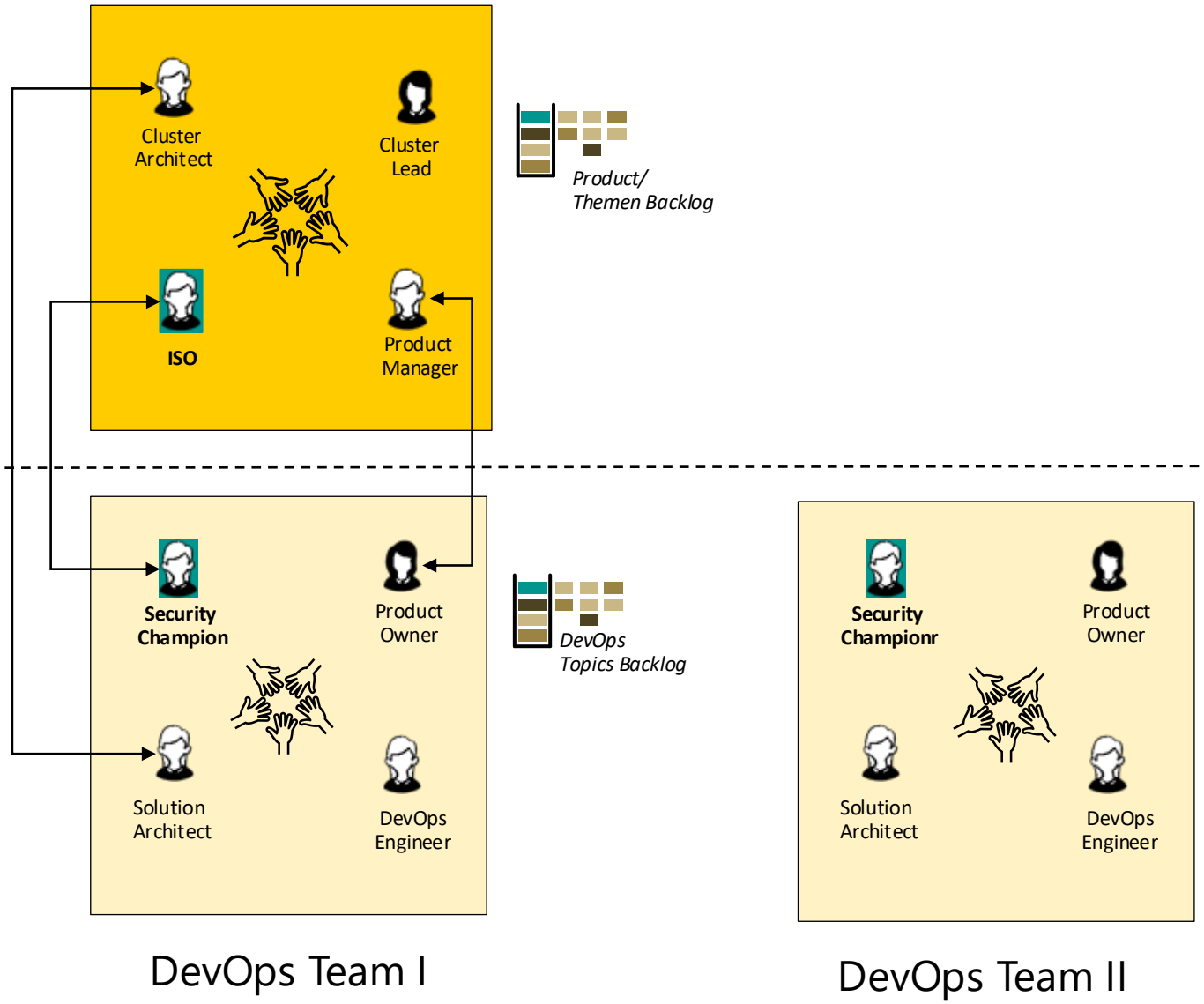
Embedded InfoSec in the Cluster

Cluster Level

ISO
- Defines the inclusion of necessary security roles
- areinformed about developments and risks
- Controls and prioritizes sec requests in the backlog
- is responsible for security documentation
- is an escalation point for the security champions
- Etc

DevOps Team Level

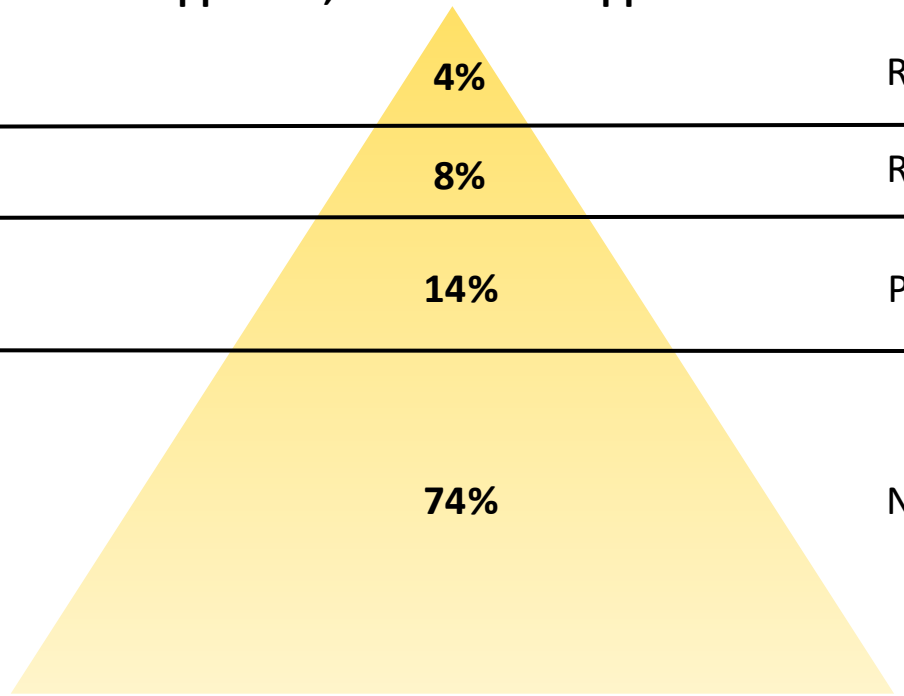
Security Champion
- Controls secure development in Dev with Sec Health Checks, Threat Modeling, etc.
- prioritizes sec requests in the backlog
- escalates to the ISO if necessary
- controls the processing of security documentation
- accompanies findings from audits and test procedures
- Among others



Deep Dive 2: Supplier Security

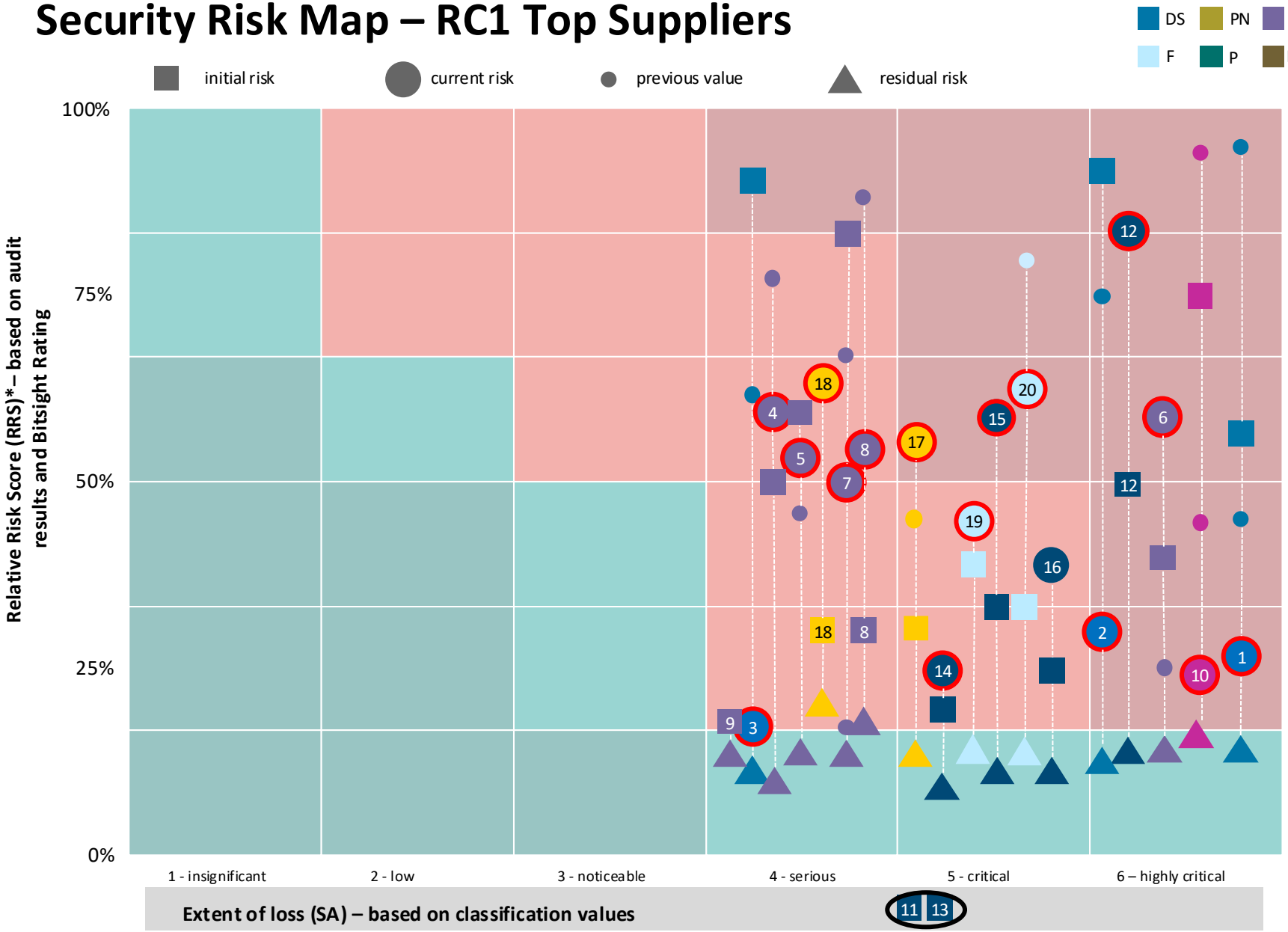
We concentrate on the suppliers that are relevant from an information security point of view and apply different measures for each risk class

Risk class	approx. 2,000 relevant suppliers*	Measures according to risk class
Risk Class 1 - Highly Critical	**4%**	Regular audits and/or pentests
Risk Class 2 - Highly Critical	**8%**	Regular Remote Risk Assessments
Risk Class 3 - Critical	**14%**	Periodic scanning for security vulnerabilities
Risk class 4 - Non-critical	**74%**	No additional measures



Legend
*Estimate at the current time of the project. **Audit -** On-site verification of security - control of contracts etc. **Pentest –** testing of technical protective measures by specialists **Remote Risk Assessment –** supplier is checked using a questionnaire

Security Risk Map – RC1 Top Suppliers



#	Lieferant	RRS*	SA**
1	Lieferant 1	60%	6
2	Lieferant 2	90%	6
3	Lieferant 3	85%	4
4	Lieferant 4	50%	4
5	Lieferant 5	60%	4
6	Lieferant 6	40%	6
7	Liefarant 7	80%	4
8	Lieferant 8	30%	4
9	Lieferant 9	20%	4
10	Lieferant 10	55%	6
11	Lieferant 11	tbd	4
12	Lieferant 12	50%	6
13	Lieferant 13	tbd	5
14	Lieferant 14	15%	5
15	Lieferant 15	tbd	5
16	Lieferant 16	25%	5
17	Lieferant 17	60%	5
18	Lieferant 18	30%	4
19	Lieferant 19	45%	5
20	Lieferant 20	95%	5

*** RRS**

1) RRS is 100% defined by Bitsight Divergences/Suppliers (bad, warn and good)
2) Audited: The RRS is defined by the number of divergences of the audit based on Bitsight

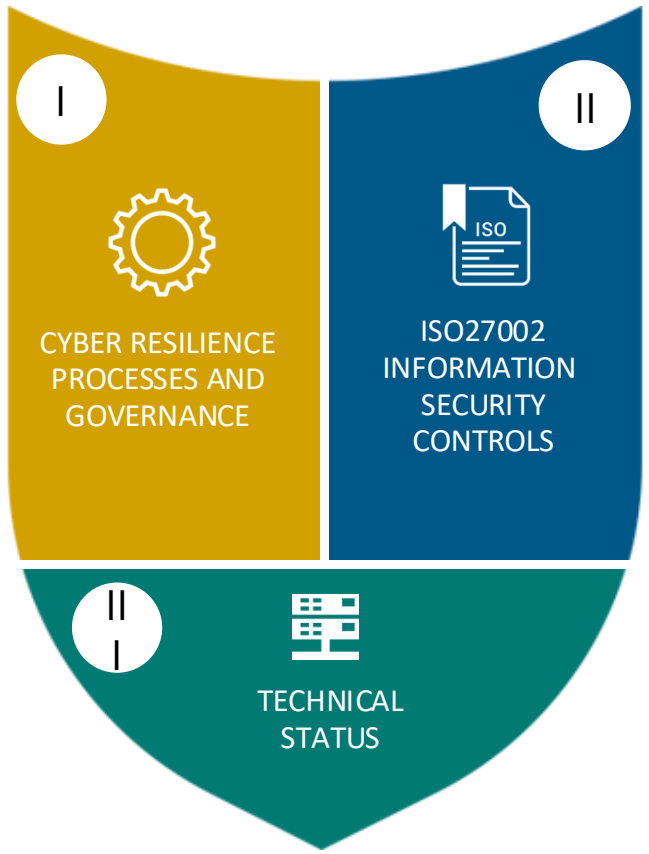
**** SA:** Ranking based on classification criteria

Classification methodology Audit (based on the number of divergences)

1) 1-3 Prio 1 divergences consequently RRS increment by 1 grade
2) (>3 - 5) Prio 1 divergences consequently RRS increment by 2 grades
3) >6 Prio 1 divergences conseqently RRS increment by 3 grades
4) 5-10 Prio 2 divergences conseqently RRS increment by 1 grades
5) >10 Prio 2 divergences conseqently RRS increment by 2 grades

Methodology

Three aspects of the Cybersecurity Matura



Cyber Resilience Maintenance Lifecycle

The CRML is a good practice from practice and enables a holistic view of the maturity in terms of processes and governance.

ISO27002 IT Grundschutz der Post

Swiss Post's IT baseline protection was analysed and simplified to meet the needs of SMEs.

Technical Status Highway Tool

In order to assess the current technical status of the SMEs, the "Autobahn" tool of the post office was used.

A 360-degree view

By applying three different methodologies, it was possible to create a holistic assessment of the maturity with regard to cybersecurity.

Assessment: I. Processes and Governance

- General organization
- Identification of hazards
- Risk assessment
- Definition of measures
- Implementation of solutions
- Testing Effectiveness

1. Basis

Details

Processes, activities or internal controls are carried out on an ad hoc basis, are person-dependent, undocumented, incomprehensible and not very reliable.

Effect

High potential for errors, higher costs due to inefficiencies, not sustainable.

2. Informal

Details

Processes, activities or internal controls are in place, but not standardised and only partially documented and therefore not traceable. Specifications are partly available, but not up-to-date and updated.

Effect

Processes, activities or internal controls as well as the updating of specifications are highly dependent on individuals.

Target bacc[illegible]reate

3. Standardized

Details

The process landscape and business processes, including controls, are documented.

Specifications are up-to-date, but are not systematically improved and may therefore have shortcomings.

Processes, activities or internal controls carried out are traceable.

Effect

Compliance, efficiency and effectiveness of processes, activities or internal controls are not monitored by the line.

4. Monitored

Details

The principles of how processes, activities or internal controls are to be operated are described in detail.

Specification documents are improved and updated annually.

Effect

Compliance, efficiency and effectiveness of processes, activities or internal controls are monitored by the line by means of key figures.

5. Optimized

Details

Specification documents, processes, activities or internal controls correspond to "best practice" and are constantly improved through benchmark comparisons.

Effect

Compliance, efficiency and effectiveness of processes, activities or internal controls are monitored in real time and with key figures, ensuring a competitive advantage.

Maturity

- Organizational
- Infrastructure
- Environment

Evaluation: II. Information security controls

35 checks in 12 categories

Information Security Policies	Organization of Information Security	Human Resources Security	Asset Management
Access Controls	Physical and Environmental Security	Operations Security	Communications Security
Systems Acquisition, Development and Maintenance	Supplier Relationships	Information Security Incident Management	Compliance

Scale

Fulfilled
The requirements according to ISO27002 are currently met.

Partially fulfilled
The requirements according to ISO27002 have been partially met.

Not fulfilled
The requirements according to ISO27002 are not met.

The audited controls are a selection of controls. Thus, this audit does not cover 100% of all controls according to ISO27002.

Evaluation: III. Technical Weaknesses

- Autobahn is a vulnerability scanner developed and maintained by globally recognized ethical hackers and security experts from Security Research Labs.
- Swiss Post is actively using this tool and is also reviewing its own infrastructure

Relevant aspects of information security	Unnecessary Exposure - Unnötiges Risikopotential	Missing Patches – Fehlende Patches	Insufficient Hardening – Insufficient Configurations, Hardening
Best-Practice	**Provide minimal services to hackers**	**Install security updates regularly**	**Configure assets securely**

Probability of a cyber security attack		
	x8	Critical A fix must be done immediately
	x4	Striking: The correction should be carried out as soon as possible
	x1	Note: The specifications should be checked and corrected according to ISO27002

Definition:

- The Hackability Score is the sum of the problems exposed via the Internet, multiplied by their severity class
- If a problem type is present multiple times, each additional occurrence will be weighted less to account for the decreasing return from the hacker

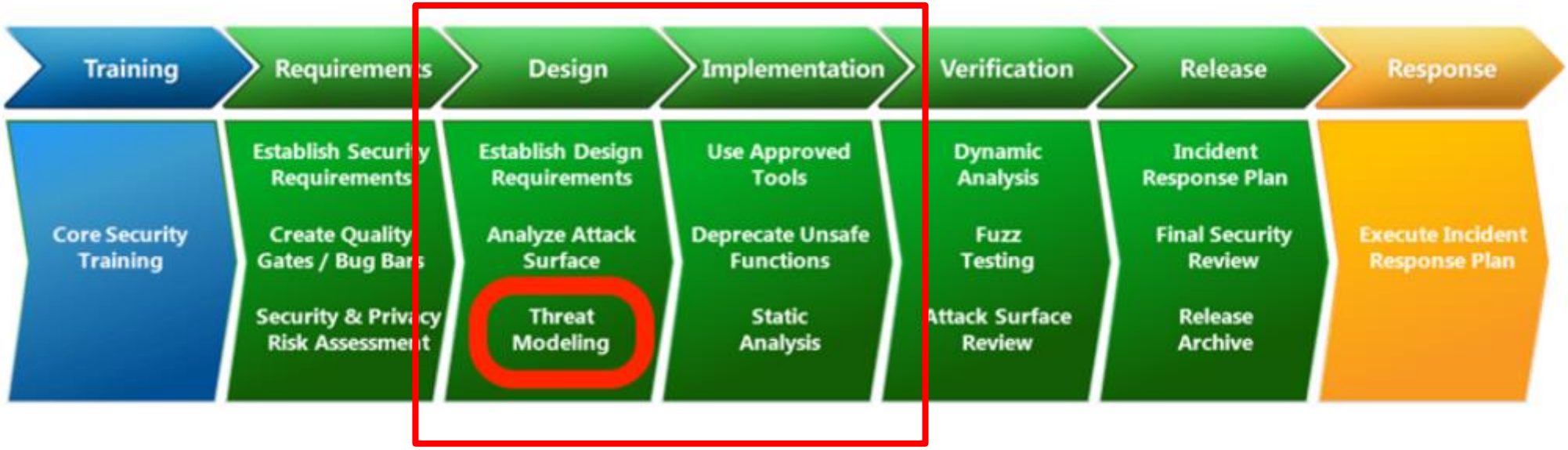
Overview

- Who are we and why
- Customer Centricity – Digital Trust
- Resilience – Participatory Security
- **Cyber Riskmgmt – Beyond**
  > Threat Modelling and Fair
  > What lies beyond

Case Study – Threat Modelling (1/3)

Method for risk treatment/communication in development

Threat modeling is best placed in the design phase



Case Study – Threat Modelling (2/3)

General Approach

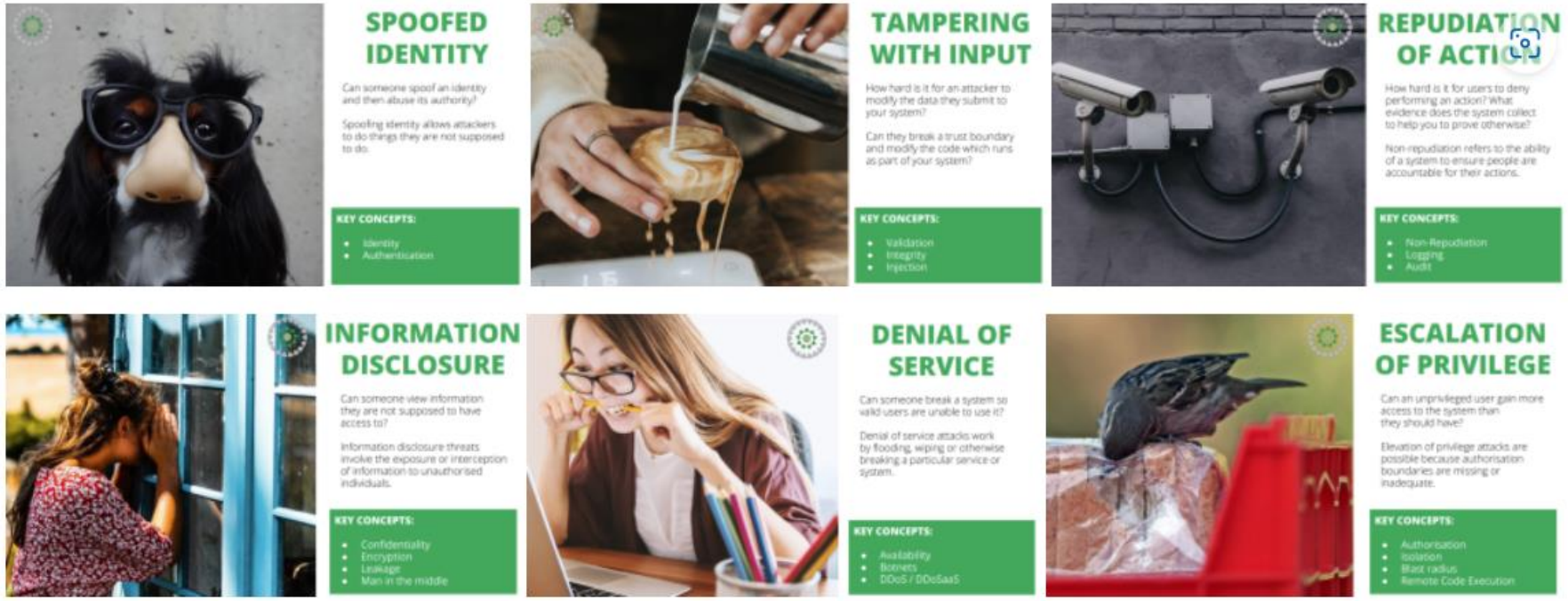
Case Study – Threat Modelling (3/3)

STRIDE - Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Escalation of Priviledge

Give every threat a priority by rating the risk

Can be as easy as Low/Medium/High based on your gut feeling

Models help to rate more consistently



BoD Example - Cybersecurity Risk Exposure

Effectiveness of measures and transparent communication

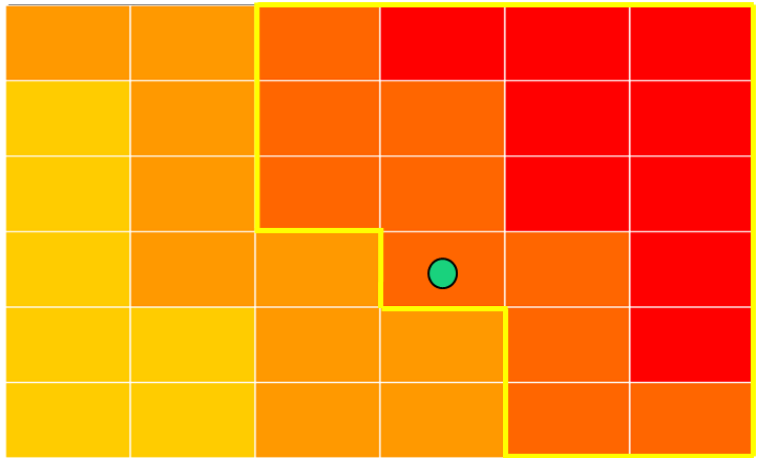
Cyber Risk Post – Calculated using credible worst case method. Scenarios including various topics, e.g. ransom attacks

Ransom Attacks – becoming complex and aggressive. Victims no longer willing to pay and aggressors publish data more frequently. Targets are office IT and increasingly production lines

Swiss Post has a solid defense dispo and a no-pay policy. We focus on recovery and proactive communication

Effective measures – ao offline backup, anomaly detection for OT, security for SMEs and bug bounty programme

Outlook – Increasing complexity of management of ecosystems, cloud, SME, carve outs, artificial intelligence



Side 35

FAIR – Factor Analysis of Information Risk
Example of Impact of complex attack scenario

	Market 1	Market 2	Market 3	Market 4
Productivity / impact on turnover *[KCHF]*	0	15’884	13’500	22’917
Reaction, Expenses in IT *[KCHF]*	8’553			
Replacement and reinvestment IT	1’152			
Cost on reputation *[KCHF]*	2’679	0	6’500	9’199
Juristic and regulatory related cost *[KCHF]*	0	500	5’000	0
Loss of competitive advantage *[KCHF]*	15’418	7’942	10’000	0
Total per market *[KCHF]*	**18’097**	**24’326**	**35’000**	**32’116**

Rule of Thumb Cost of an incident 10 times higher than investment in protection

Overview

- Who are we and why
- Customer Centricity – Digital Trust
- Resilience – Participatory Security
- **Cyber Riskmgmt – Beyond**
  > Threat Modelling and Fair
  > **What lies beyond**

Technological Edge

Cryptographic Agility

Identity-Centric Security

Attack Surface Morphing

Agent Based Defence

Virtual Citizenship / Personhood

Welcome to the Mirror Dimension

The Magic has begun