PERSONAL INVITATION to 27th

swissciso summit

Reporting and Risk Communication: What are good approaches based on experience?

31st January 2023, Zunfthaus zur Schmiden, Zürich
(upon requests, virtual participation will be organized)

Sponsorships:

DETECON CONSULTING — Platinum

pwc — Gold

FUB | Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN | SWITCH — Silver

paloalto NETWORKS | SWISS POST

Partner:

satw it's all about technology

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 27th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Please be informed that we have only a limited number of places. Therefore we kindly ask you to confirm your attendance as soon as possible.

Prof. Dr. Bernhard M. Hämmerli

Reporting and Risk Communication: What are good approaches based on experience?

Date	31st Janurary 2023
Time	12:00 Lunch and 13:00 Summit starts / approx. 19:00 Summit ends
Location	Zunfthaus zur Schmiden Marktgasse 20, 8001 Zurich, Switzerland Please contact Prof. Dr. Hämmerli for virtual participation.
Keynote 1	**Compliance or Risk Reporting? The answer is "Yes!"** Frank Heinzmann, Global Head of Cyber & Information Security Risk Control at UBS
Sharing among peers	**How to address the Executive Board and Board of Directors?** Marcel Zumbühl, CISO Swiss Post, Member of IT-Board Post and BOD Member of Hacknowledge
Keynote 2	**Using Risk Quantification – Lessons from the trenches** Philippe Vuilleumier, Senior Security Advisor at Swisscom
Key Benefits	· Experience industry best practices in the Swiss market · Participate actively in moderated high-level peer exchange · Understand drivers for security, gain competence and experience in discussing strategic issues · Design, develop and manage effective information security strategies for your own organisation · Receive an exclusive consolidated end of summit report detailing all the major themes discussed for re-use in your organization

Join the Swiss CISO Summit and benefit from the peer exchange!

Summary 2

Reporting and Risk Communication: What are good approaches based on experience?

It is very simple: CISOs need more security investments to improve security.

Decision-makers want to innovate businesses and create more revenue. In this role, decision-makers must be risk-takers: no risk means no new business. On the other hand, CISOs feel responsible for the company's security and hate to have serious incidents. The anger would be even higher if a serious incident could be avoided with a recently rejected security project proposal. And the natural tendency of CISOs is to be risk averse. CISO must be aware of this opposing attitude of the decision-makers.

In the analysis of optimizing this ecosystem, there are two tools CISOs are using:

Reporting: This is how decision-makers receive information: There was sufficient education for them, and they know how to process the information.

Risk communication and reporting: Cyber risks are not in the core competence of decision-makers. And cyber risks are competing with many other risks for funding. The usual way of risk evaluation, likelihood, and anticipated damage is somewhat shaky because it is often a quite heuristic approach. Science and companies are developing new tools for making the risk assessment process more transparent and with better traceability. Does this change the mind of the decision-maker? Of course, there is still a gap between formal risk and business impact. But only business impact is relevant for decision-makers, and CVSS vulnerability scoring does not usually trigger any action.

Addressees of these efforts are board and executive management. Both addresses have different roles, and we want to elaborate on these roles and the variation between the various companies that will be present.

This summit aims to enrich each other with strategies, a successful mix of reporting and risk communication, and a topic and methodologies that look great but could be better in this context. Marcel Zumbühl will open the board perspective. We can learn how to prepare the communication with the most important facts and eliminate all that bothers the decision maker but has no real effect.

As a result, we hope less work will result because prepared information is more targeted and tuned to the decision maker. And probably, in some cases, also a new dimension of humility because we have better acceptance and understanding of the decision maker's views.

3 Keynote I and Roundtable I

Keynote I

Compliance or Risk Reporting? The answer is "Yes!"

Compliance reporting ("Do I comply with laws, rules, and regulations?") has become increasingly popular in recent years, mainly to satisfy expectations from regulators and authorities. But is it what the CISO needs? Isn't articulating the current residual risk a stronger tool to prioritize actions, workforce, and investments ("How big is the problem?")? Which metrics, indicators, and tools can help a CISO to aggregate such a risk view in the reporting hierarchy without losing sight of compliance aspects? Frank will open his perspective on these questions in his presentation and put various reporting methods into perspective.

Roundtable Session I

Risk reporting and compliance: how to create a maximal effect for better security?

Compliance reporting is aligned with the way how executives are steering the company. There is little room for interpretation since the law must be complied with; otherwise, there are serious consequences for the responsible managers and executives. Risk reporting is written in the language of security engineers and is the primary reporting tool for a line of defense 1 (and 1.5). The community understands each other well. However, decision-makers are usually Risk-taking and not Risk-averse. And they do not mind risk when no substantial business impact is associated with it.

We want to elaborate on the experience exchange of the optimal mixture when we should use tools for compliance and when tools for risk reporting). And, of course, both compliance and risk reporting are always active, which creates good opportunities for the CISO to create a double strategy with a fine-tuned mix of both. The success of this mix is part of how CISOs are measured.

Frank Heinzmann is Global Head of Cyber & Information Security Risk Control in UBS, based in Zurich. In the past 30 years, Frank held various positions in multinational companies in the fields of Information Security Governance, Risk, Audit and Compliance. Furthermore, he is a long-standing board member of the Information Security Society Switzerland (ISSS) and is lecturing “Security Governance & Compliance” at the Lucerne University of Applied Sciences and Arts. Frank owns ISACA´s CGEIT Certificate.

Sharing among peers

4

How to address the Executive Board and Board of Directors?

Executive Boards and Boards of Directors work on different levels. While the first is tasked with running the company the latter is responsible for strategy and oversight. CEOs and executive boards are meeting frequently whilst BoDs as a rule meet-up 4-6 times a year. There is a large information divide between the two committees, but BoDs must be able to determine if their company runs well both financially and as well as compliance-wise. This is where you as a CISO come into play. The days are over, when CISOs knocked on the door in vain, now have a seat at the table and can contribute to the success of your company at board level. Lets find out how you can make the most of it.

Marcel Zumbühl works for Swiss Post as Chief Information Security Officer (CISO) and member of the IT Board since August 2018 and is responsible for the information security in the Group. He joined the Board of Directors of Hacknowledge SA in 2022. The 52-year-old holds a master degree in computer science with a minor in business administration. After studying at the University of Berne, he worked both in Switzerland and abroad for various companies such as Accenture, Swisscom and Credit Suisse. Marcel lectures at ETH Zurich and HSLU on risk communication as well as CISO issues and is Co-President of the Information Security Society Switzerland (ISSS).

5 Keynote II and Roundtable II

Keynote II

Using Risk Quantification – Lessons from the trenches?

CISOs are faced with many challenges, including cyber risk management. It's accepted practice that a risk-based approach is useful when prioritizing these challenges. This immediately raises questions concerning the treatment of these risks. How are they identified, evaluated, prioritized, communicated, and managed during their lifecycle?
At Swisscom, we started making our first steps with risk quantification using the FAIRTM (Factor Analysis of Information) methodology in 2020. The assumption was that understanding these risks across the company would improve if we could assign a monetary value to cyber risks. This, in turn, should lead to implementing the necessary mitigating measures more quickly, thereby reducing the company's risk exposure.
The presentation's content concerns whether this assumption has proven true and what lessons were learned with risk quantification.

Roundtable Session II

Which risk communication and risk reporting have the best effects for reaching higher security

Convince boards and executive management to more expenses in information security is the goal of CISOs.
Why are decision makers somewhat reluctant to the CISO? Do they concentrate on business impact instead of risks, or are they just better risk takers than the CISO, which usually are risk-averse?
Can we improve risk analysis methodology with quantification and receive different results? Are other Communication tools better? Or is the security budget given, and the decision-makers do not want to spend more?
And in the always ongoing relationship management with decision makers, when should we be "nice" and when should we be "Challenging" to reach the best results?

Philippe Vuilleumier has worked at Swisscom for more than 15 years and had overall responsibility for Swisscom Security as Head of Group Security from September 2015 to December 2022. He was Head of Network & IT Operations at Swisscom Switzerland from 2008 before being appointed CEO of subsidiary Alphapay in 2013. Since January 2023, he has been leading various projects to enhance Swisscom's security further in his new role as Senior Security Advisor.

Before joining Swisscom, Philippe Vuilleumier held various management positions at Zurich Insurance Group, Equant, and IBM.

His qualifications include a master's degree from the Delft University of Technology in Business Telecommunications.

Philippe is currently on the Board of Directors of Electrosuisse, participates actively in several organizations related to physical and cybersecurity, and served as President of the Board of Directors of SEC Consult Switzerland AG.

Information 6

What is the Swiss CISO Summit?

The Swiss CISO Summit facilitates the exchange of current security challenges and opportunities between security executives, managers, and thought leaders in Switzerland. Each summit addresses a current hot topic. The strategic dialog and the subsequent discussions are inspired by a keynote speech from well-recognised national and international speakers. The moderated and guided discussions in groups of 8-10 members share views, experiences and strategies. An excerpt of the discussions will be written down in the result paper for the participants.

Participation is by invitation only.

How Swiss CISO Summit maintains confidentiality?

The Swiss CISO Summit is provided as a closed-door event (please contact Bernhard Hämmerli for participation). This exclusive CISO Executive programme is created for information security and risk executives providing them with an environment for achieving new ways of thinking and ensuring success in protecting their organisations.

The summits are held strictly under the Chatham House Rules which is the ruleset to treat the shared information with full discretion, and for providing secrecy against non-group persons.

Why should I join the Swiss CISO Summit?

The Swiss CISO Summit has a unique concept of creating trusted circles amongst executives,managers and thought leaders. Meeting peers in an advanced business location, having time to network amongst each other and to touch current issues which are unique opportunities for sharing experiences, and for receiving advice far beyond the discussion at the table.

- Extensive networking opportunities with peers and experts on an ongoing basis
- Meet with other leading executives to share successes, failures, obstacles, and challenges
- Learn about current strategies on managing security threats and to prepare for the future
- Make new connections and equip yourself with information on recent projects and achievements

What makes the difference?

The Swiss CISO Summit has many and diverse benefits for the invited experts. The participants are the focal point of the summit and the meeting is not intended for providers to present solutions or products. Sales are strictly prohibited to the good of an open and free CISO information exchange.

What is the history behind the Swiss CISO Summit?

The Swiss CISO Summit has been run successfully since 2001 under the name «Risk and Security Exchange» and from 2004 - 2009 when it was known as „Swiss Security Exchange“. Then with the financial turmoil the summit came to a halt. From 2009 onwards, the same successful format was adopted in Norway where it ran under the name „Sikkerhetstoppmøte“. All this experience gained by Prof. Dr. Hämmerli is put into the organisation of the Swiss CISO Summit.

6 Information

Who prepares and facilitates the Swiss CISO summit?

An organising committee under the lead of Prof. Dr. Bernhard M. Hämmerli is responsible for the invitation, preparation and guidance of the discussions. He is an internationally well recognised expert with 25 years of experience in information security in governments, industry and academia. He led the Cyber Security activities of the Swiss Academy of Engineering Sciences SATW from 2012 – 2017.

Prof. Dr. Hämmerli is a founding member of the Information Security Society Switzerland and he built up the first Information Security master programme in Lucerne in 1996, respectively 1999, and since 2017 he is head of the new BSc Information & Cyber Security at Hochschule Luzern/Informatik. Additionally, he teaches at the Norwegian University of Science and Technology Norway www.ntnu.no, in the technology and management track of the Information Security master programme.

Prof. Dr. Hämmerli is supported by Katarzyna Kuhn for administrative purposes.

Agenda (generalised)

12:00	Start with a small lunch
12:45	Networking Session
13:15	Welcome and introduction
13.30	Keynote from experts or members
14:00	Roundtable session I
15:00	Exchange between the groups and wrap-up of roundtable I
15:10	Break
15:40	Keynote from experts or members
16:10	Roundtable session II
17:05	Exchange between the groups and wrap-up of the roundtable II
17:15	Summary note
17:30	Cocktail and aperitif
19:00	End

The meeting is held three times per year.

Registration 7

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to 40 per summit in order to maintain an atmosphere of trustful information sharing.

Single summit CHF 450.- per participant
Three summits CHF 1'000.- per participant (25 % discount for booking three consecutive summits – not three participants at the 25th summit)

Cancellation Policy

Cancellations of registrations are free of charge only if received no later than seven days before the summit. Cancellations received beyond this point will incur 100 % of the admission fee. In any case a delegate may be sent at no additional cost. More information is found at www.ciso-summit.ch. Content responsibility for the summits lies with Prof. Dr. Bernhard M. Hämmerli.

Register by just replying to the invitation email with all your details or by following these steps:
Step 1: Fill out & save the form
Step 2: Select Send button > email opens (info@ciso-summit.ch)
Step 3: Attach the PDF file

Registration

PRINT RESET SEND

Register by just replying to the invitation email with all your details – or by filling out this form and mailing it to info@ciso-summit.ch.

☐ **Three consecutive summits for CHF 1'000.–**
3 Summits, Summit 27 (31.1. 2023), 28 (09.05.2023), 29 (24.10.2023)

☐ **27th Swiss CISO Summit:**
31.01.2023: CHF 450.– for all forms of participation

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ *Date* _____

8 Sponsorships & Partner

Platinum Sponsor — **Detecon**

Detecon Consulting is one of the world's leading management consulting companies for integrated management and technology consultancy. Detecon (Schweiz) AG is located in Zurich and bundles Financial Management as well as ICT Management competences among its roughly 150 employees. The main focus lies on the requirements of CFOs and CIOs in nearly all industry sectors.Globally, more than 6000 projects have been implemented successfully. The international spirit and the openness are reflected not only in the number and origin of our clients from over 160 countries but also in our employees that are recruited from 30 different nations.

Gold Sponsor — **PricewaterhouseCoopers**

At PwC, our purpose is to build trust in society and solve important problems. PwC looks at cyber security as one of the biggest challenges to solve in today's times and provides a full stack of cyber security consulting services. PwC's Cyber security practice comprises deep information security, forensic technology, business and technology resilience, Cybercrime response, technology risk and controls, project and program management and operations specialists to help clients address Cyber risks through the whole lifecycle from strategy to execution and operations.

Silver Sponsor — **SWITCH FOUNDATION**

The foundation "SWITCH" was founded in 1987 under private law by the Swiss Confederation and the university cantons and is an integral part of the Swiss-academic community. Based on our core competencies network, security and identity management, SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment. SWITCH's Computer Emergency Response Team (SWITCH-CERT) is one of the most experienced CERT and besides the government CERT MELANI, one of two National CERTs in Switzerland.

Silver Sponsor — **Armed Forces Command Support Organisation (AFCSO) Führungsunterstützungsbasis (FUB)**

With its services in ICT and electronic operations, the Armed Forces Command Support Organisation (AFCSO) ensures that the armed forces can accomplish their missions. It guarantees the command and control of the armed forces under all conditions.

Silver Sponsor — **SWISS POST**

Swiss Post is part of the critical infrastructure of Switzerland. On top of its logistics and transport services, Swiss Post offers a variety of digitalized services in other industries ao. electronic voting, eHealth and secure eMail. The ICT department holds certificates on ISO 27001, 22031 and 20000. Information Security is an integral part of all activities of Swiss Post Group. As a first mover in the Paris Call for Security and Trust in Cyberspace, Swiss Post Group fosters expertise sharing on security in trusted environments both nationally and internationally.

Sponsorships & Partner

8

Silver Sponsor	**HSLU**
Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN	Lucerne School of Computer Science and Information Technology provides most comprehensive range of IT study programs within Switzerland. The Lucerne School of Computer Science and Information Technology offers bachelor's and master's degree programs, applied research and development, and continuing education programs in Computer Science, Information Technology and Business Information Technology. Newly developed (past 5 years) and innovative study programs are: Information & Cyber Security, Artificial Intelligence and Machine Learning, Digital Ideation, and International IT Management.
Silver Sponsor	**Palo Alto**
paloalto NETWORKS	Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.
Partner	**SATW**
satw it's all about technology	SATW is recognized as the Swiss organization for the communication of independent, objective, and comprehensive information about trends in technology – as a basis for the forming of well-founded opinions – and as an effective institution for the promotion of engineering sciences and new technologies in Switzerland. SATW identifies technological developments of relevance to industry and informs politicians and society about the significance and consequences of such developments.

swissciso summit

More information is found at www.ciso-summit.ch

Sponsorships:

DETECON CONSULTING

Platinum

pwc

Gold

HOCHSCHULE LUZERN

SWITCH

Silver

paloalto NETWORKS

SWISS POST

Partner:

satw it's all about technology