

PERSONAL INVITATION to 34<sup>th</sup>

swiss**ciso**summit



## Business-focused Cyber Security as a Competitive Advantage – how does this really look and work?

13<sup>th</sup> May 2025, Zunfthaus zur Schmiden, Zurich  
(upon requests, virtual participation will be organized)

Sponsorships:



Platinum



Gold



Lucerne University of Applied Sciences and Arts  
**HOCHSCHULE  
LUZERN  
SWITCH**

Silver



Partner:

**satw** it's all about technology

# Contents

**1**

Introduction

*Page 3*

**2**

Summary

*Page 4*

**3**

Keynote I and  
Roundtable I

*Page 5*

**4**

Keynote II and  
Roundtable II

*Page 6*

**5**

Information

*Page 7*

**6**

Registration

*Page 9*

**7**

Sponsorships &  
Partner

*Page 10*

# 1

# Introduction

**Dear CISO,**

You are kindly invited to the 34<sup>th</sup> 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



## Business-focused Cyber Security as a Competitive Advantage – how does this really look and work?

**Date** 13<sup>th</sup> May 2025, zur Schmiden, Zurich  
**Time** 12:00 to 19:00h  
**Location** In-person: Zunfthaus zur Schmiden, Marktgasse 20, 8001 Zurich

**Keynote 1** **Crazy incentives, how they kill security: What is your role to turn the wheel?**  
Christian Folini, Security Engineer, Keynote Speaker, Moderator, netnea.com

**Keynote 2** **Before and after the booking.com incident:  
How we live now with business-focused and business-aligned security.**  
Sascha Maier, CISO SV Group, Zurich

- 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

## **Business-focused Cyber Security as a Competitive Advantage – how does this really look and work?**

Information and cyber security develop nearly every second year with a new mindset: Initially, in the eighties, Cryptographers were the real security experts, awareness specialists took over, network security, system security, and many more mindsets were predominant. Today we know that all aspects together make the security orchestra.

One essential aspect always remained: security should serve the business and protect the business along with its needs. The business did not care for too long and thought the engineers should make all save. It happened because of the complexity of security and the large language gap between engineers and managers. Business-focused means that the business knows which security aspects are relevant and impact the business and which properties are important for the engineers but not relevant for the business.

In the new area, very rich private customers want to speak to banks' IT security personnel and know whether their money is well protected. The customers are accompanied by cybersecurity experts who perform the due diligence security checks.

It is just an example of competitive advantages resulting from high-end protection.

Through cybercrime, we face enormous damages that set our prosperity and welfare at risk: Germany reports losses (including secondary issues at a standstill) of 266 billion euros in 2024. The overall global loss would be ranked 3 in the nation's GDP ranking, just after the USA and China. Against this background, cyber security is essential, and top business-focused cyber security is a competitive advantage.

Christian Folini, we will experience business conditions that align with security and business incentives that weaken the overall security. Sascha Maier, CISO SV Group Zurich, will present how an incident can turn around the situation, what it means to align security to business, and how this can be implemented successfully.

As usual, we will provide two debates:

- Discussion Round 1: **What is "bad" & "good" security, and how to create the best conditions for using always the best viable option?**
- Discussion Round 2: **Business aligned and focussed security: What are the core elements, and how to implement the concept successfully?**

# 3

## KEYNOTE I AND ROUNDTABLE I

### Keynote I:

#### Crazy incentives, how they kill security: What is your role to turn the wheel?

Everybody is driven by incentives. Good incentives persuade us to do the right thing and patch our servers. Bad incentives make us eat unhealthy food and follow stupid security practices.

There is a huge resource problem in IT, especially in the IT security industry. Therefore, you would expect people to pay attention to the existing incentives and the ones they create with their budget allocation, their awareness training, their security reports, etc.

But reality paints a different picture: Bad incentives all around! We see insane security practices eating valuable time and online training annoying corporate users.

But it's even worse. I've come across incentives that lure companies into creating bad products, and I've seen companies create products that incentivize their customers to waste their time.

It takes people like you and me to say "NO" and stand up for real security!



**Christian Folini** is a Swiss security engineer and open-source enthusiast. He holds a PhD in medieval history and enjoys defending castles across Europe. Unfortunately, defending medieval castles is not a big business anymore, so he turned to defending web servers, which he finds equally challenging. He brings 15 years of experience with ModSecurity configuration in high-security environments, DDoS defense, and threat modeling. Christian Folini is the author of the second edition of the ModSecurity Handbook and the best-known teacher on the subject. He used to co-lead the OWASP ModSecurity Core Rule Set project and serves as the program chair of the "Swiss Cyber Storm" conference. In 2024, the Swiss government invited him to join the Swiss National Cyber Strategy Steering Committee. Christian Folini is a frequent speaker at conferences, where he tries to use his background in the humanities to explain hardcore technical topics to audiences of different backgrounds.

### Discussion Round I:

#### What is "bad" & "good" security, and how to create the best conditions for using always the best viable option?

# KEYNOTE II AND ROUNDTABLE II

## Keynote II:

### Before and after the booking.com incident: How we live now with business-focused and business-aligned Security

In today's digital landscape, the hospitality industry has become a prime target for cybercriminals. Incidents involving major platforms such as Booking.com, Expedia, and Airbnb have surged dramatically, underscoring the urgent need for robust cybersecurity strategies.

New security strategies have been implemented in response to these incidents, focusing on overcoming industry-specific challenges. A significant concern is aligning security protocols with hotel staff who are often underpaid, may have limited formal education, and work in high-stress environments.

Furthermore, methods to seamlessly integrate security measures with business objectives are being explored, ensuring that security enhancements contribute to overall business growth. Strategies to position security as a credible competitive advantage are also being developed, effectively communicating its value to stakeholders.

The evolution of security approaches in the hospitality sector is evident, especially as businesses recognize security as a fundamental component of their value proposition. These developments offer valuable insights for professionals aiming to comprehend and implement cybersecurity measures that align with business goals in the hospitality industry.



**Sascha Maier** is the Chief Information Security Officer (CISO) at SV Group in Zurich, a leading gastronomy and hotel management organization with divisions spanning community restaurants, public catering, hotel management, and digital solutions. Before this, he dedicated over a decade as the Head of IT & Cyber Resilience at IWC Schaffhausen, the renowned luxury watchmaker, overseeing comprehensive IT and information security across all its locations. In addition to his industry roles, Maier contributes as a lecturer at the University of St. Gallen (HSG) and serves on the advisory board of the Swiss Cyber Institute, Harmonic Security, and Smarttech247. Recently, he authored "Business Risk Cyber-Security – Guide to Establishing a Resilient Security Ecosystem," a book that offers foundational insights into potential cybersecurity threats and provides guidance on developing a robust security framework.

## Discussion Round II:

### Business aligned and focussed security: What are the core elements, and how to implement the concept successfully?

## 5

## Information

**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.

# Information

# 5

## 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](http://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.



# 6

## Registration

### 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 31<sup>st</sup> 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](http://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](mailto:info@ciso-summit.ch))

Step 3: Attach the PDF file

### Registration

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](mailto:info@ciso-summit.ch).

#### Three consecutive summits for CHF 1'000.–

3 Summits, Summit 34 (13.05.2025), 35 (28.10.2025), 36 (27.01.2026)

#### 34<sup>th</sup> Swiss CISO Summit

13.05.2025: CHF 450.- for all forms of participation

First Name \_\_\_\_\_ Surname \_\_\_\_\_

Organisation \_\_\_\_\_

Street / No. \_\_\_\_\_ ZIP / City \_\_\_\_\_

Phone \_\_\_\_\_ Email \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_



# 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**

**SWITCHFOUNDATION**



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) Cyber Command**



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.

# 7

## Sponsorships & Partner

### 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.

### 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.

# swisscisosummit

More information is found at [www.ciso-summit.ch](http://www.ciso-summit.ch)

Sponsorships:



Platinum



Gold



Lucerne University of Applied Sciences and Arts

HOCHSCHULE  
LUZERN  
SWITCH

Silver



Partner:

