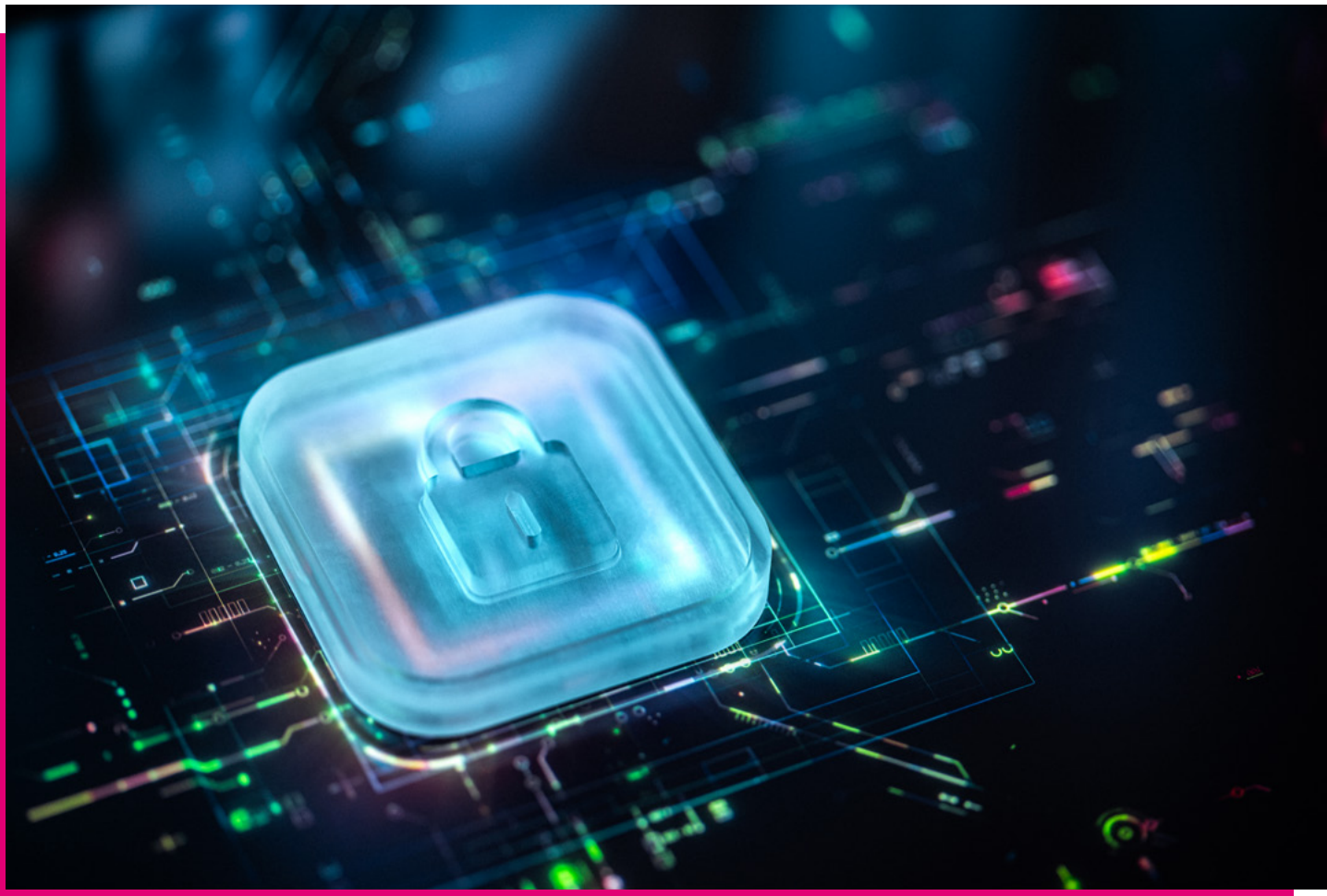
Personal Invitation to 35th

swisscisosummit



Cybersecurity risk management – A new area of Cyber Transparency?

28th October 2025, Kursaal Berne, Bern
(upon requests, virtual participation will be organized)

Sponsorships:

Detecon — Platinum

pwc — Gold

Hochschule Luzern — SWITCH — Silver

SWISS POST

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 35th 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

Cybersecurity risk management – A new area of cyber transparency In-person, (upon request virtual participation will be organized)?	
Date	28th October 2025, in-person Kursaal Berne, Bern
Time	9–19h with Cyberstorm visit, CISO Summit only: 12:15 to 19:00h
Location	Kursaal Berne, Room Panorama
Keynote 1	**Cybersecurity Risk Management: A new area of Cyber Transparency** Urs Küderli, Partner, Lead Cybersecurity and Privacy, PwC
Keynote 2	**Cybersecurity Risk Management: How to successfully implement?** Alexander Odenthal, Group Information Security Officer, Swiss Life Holding
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

Cybersecurity Risk Management – A new area of Cyber Transparency

Cyber Risk Management is the continuous process of identifying, evaluating, and mitigating threats to an organization's digital assets, data, and systems to protect against cyberattacks and ensure business continuity. It involves assessing potential risks, implementing appropriate security measures, and continuously monitoring for new threats to minimize negative impacts like financial loss, data breaches, and reputational damage. A strong Cyber Risk Management program is crucial for modern businesses due to the increasing reliance on technology and the evolving landscape of cyber threats.

Key Steps in the Cyber Risk Management Process are the same as in conventional risk management: risk identification, assessment, treatment (mitigation), monitoring, and communication.

Why do we address this topic with high priority? Digitization is the most prominent key issue for achieving more efficiency, outperforming the competition, and saving money. However, potential risk increases when raising the digitization level. Therefore, we must protect digital assets with safeguards, ensure business continuity, preserve companies' reputation, and monitor compliance, with corrective measures when deviations are detected.

In the last period, new regulations and laws have emerged, accelerating the digital transformation with new technologies, including cloud computing and remote work. These changes are very difficult to follow in-depth. In addition, we need to prepare for post-incident procedures, ensuring that in the event of successful incidents, the company can return to normal operation as quickly and effectively as possible. Another new fact is that the enterprise approach is broader and more holistic: stakeholders from IT, security, business functions, partners, and clients may be integrated.

The debates will be introduced by top speakers, and will contain:

- Round 1: **Cybersecurity Risk Management: What changes have occurred in the past strategic period, and what must we focus on for the next strategic period?**
- Round 2: **Implementing a Cybersecurity Risk Strategy: Business and Cyber Risk, buy-in, target state, design and implementation – how do you proceed?**

We are looking forward to meeting you again and having inspiring debates.

On behalf of the organizing committee, Bernhard Hämmerli

3 KEYNOTE I AND ROUNDTABLE I

Keynote I:
Cybersecurity Risk Management – A new area of Cyber Transparency

Despite the rapidly evolving digital landscape, new cyber threats, regulations, and compliance requirements, cybersecurity risks are not adequately recognized or embedded as an essential component in broader business and enterprise risk management. Level-appropriate transparency helps to protect organizational assets effectively, increases resilience strategically, and allows for adequate budget allocation, including strategic messaging at the executive level and linking operational cyber risks, controls, and metrics promoting transparency from threat identification, to assessment, to management and reporting.

Urs Küderli is a partner at PwC Switzerland and leads its Cybersecurity and Privacy practice. With over 25 years of experience in information technology and security, he is passionately involved in utilizing technology for innovative business models, helping clients safely navigate digital transformation, and ensuring the protection of their investments in the long term. With his strategic mindset and analytical expertise, he advises on building effective cyber organizations and cyber programs, as well as promoting the organization's resilience. One of the key focus areas for Urs Küderli is the integration and enablement of cyber risks into corporate risks, from business to operational cyber risk management and reporting.

Discussion Round I:
Cybersecurity Risk Management: What changes have occurred in the past strategic period, and what must we focus on for the next strategic period?

KEYNOTE II AND ROUNDTABLE II

4

Keynote II:
Cybersecurity Risk Strategy: How to successfully implement?

When designing a Cybersecurity Risk Strategy, a range of possibilities opens up. Implementation planning and execution may vary significantly, depending on the current state, organizational structure, and maturity of an organization. Different organizational structures (e. g. centralized or decentralized) change the way of achieving a management buy-in. The presentation will share successful experiences and practices. And offers hands-on insight.

One focus will be the "Recover" Function in the NIST CSF 2.0 framework that reveals its importance after a successful cyber-attack. Having the end in mind (continuous operation) means shifting attention to reliable and adequately fast recovery capabilities for being able to restore in a worst-case scenario.

Alexander Odenthal is the Group Information Security Officer at Swiss Life Holding Switzerland and leads strategic Information Security and Risk Management with a mindset of continuous curiosity and learning. Since starting in a Global Sourcing Business in 2000, I have accumulated many years of experience in IT, information security, compliance, and cyber risk management. Having worked in various sectors, his current focus is on modern cyber-resilience in a fast-evolving and volatile threat landscape. Following a risk-based approach and focusing on the availability and protection of critical assets (DORA = "critical and important functions") is the center of operational resilience. A shift from a "compliance mindset" is observed towards continuous risk management with effectiveness controls monitoring across IT infrastructures. Last, but not least, mastering cyber-resilient back-up and restore procedures for compromised or encrypted IT environments within Cyber RTO and RPO target values is a challenge that is often underestimated.

Discussion Round II:
Implementing a Cybersecurity Risk Strategy: Business and Cyber Risk, buy-in, design, target state, and implementation – how do you proceed?

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.

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 eers 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

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.

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, 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 31st 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 35 (28.10.2025), 36 (21.01.2026), 37 (19.05.2026)

☐ **35th Swiss CISO Summit**
28.10.2025: CHF 450.– for all forms of participation

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ *Date* _____

Sponsorships & Partner

7

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) 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.

swissciso summit

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

Sponsorships:

Platinum

Gold

Silver

Partner: