

Personal Invitation to 17th
swisscisco summit

Security Culture:
How to measure, change and optimize?

15th October 2019 in Bern

DETECON
CONSULTING

pwc

SWITCH



SWISS POST

Sponsorships:

Platinum

Gold

Silver

Contents

1	Introduction	Page 4
2	Summary	Page 5
3	Session I	Page 6
4	Session II	Page 7
5	Information	Page 8 – 9
6	Sponsorships	Page 10
7	Registration	Page 11

Introduction

Dear CISO,

You are kindly invited to the 17th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Unfortunately we only have a limited number of places, therefore we kindly ask you to confirm your attendance as soon as possible.



Prof. Dr. Bernhard M. Hämmerli



Security Culture: How to measure, change and optimize?

Date 15th October 2019

Time 12:00 Lunch and 13:00 Summit

The Swiss Cyberstorm program starts at 8:30h.
(Networking with VIP party of Swiss Cyberstorm – Starting 18:00 Free Entrance offered by Swiss Cyberstorm)

Location Kursaal Bern

Kornhausstrasse 3, 3000 Bern, Switzerland

Keynote I **Swisscom's Security Culture for business, Cloud and Mobility:
Change, Success Factors and Implementation**
Philippe Vuilleumier, Head of Group Security, Swisscom AG

Keynote II **Security Culture in SBB's Digitization Process:
Analysis, Operational and Strategic Targets**
Jan Hohenauer, Deputy Chief Information Security Officer, SBB AG

- 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

Security Culture: How to measure, change and optimize?

Culture could be considered as “the ideas, customs, and social behavior of a particular people or society” and represents commonalities of specific groups of people, including beliefs in specific values. Typically, most people think that culture is rather static than dynamic.

Our observation of the recent past depicts fast changes in technological and communicative means such as the internet, smartphones, group building (including on-line groups), innovation and societal integration. An additional factor is the seamless mixture of societies, such that we work today naturally in teams from many nations, while 50 years ago, we immediately felt a difference, even from people of another city in Switzerland.

As a security officer, we are concerned with all three issues simultaneously: fast changes, a seamless mixture of people with different origin, and nearly any mixture of beliefs and values. Without governance and clear direction, companies might develop a nearly unlimited number of very different odd subcultures. Now begins our tasks to care for a forward-directed and agile security culture, which adapts continuously to new situations.

We will get a report from Swisscom (main issue: business IT, Mobility, and cloud) and from SBB (Main issues OT, digitization, industrial control systems), and how they approach this enormous challenge. First turn around the employees to accept net technology, processes and human interaction, and then demand on top of these aspects a new security culture. How to keep motivation at a high level, create identification with the security controls, and protect the IPR and the data? How to measure these aspects, and how to select the best option in specific situation for well-defined change program? Now we welcome you in the world of the 17th Swiss CISO Summit.

3

Session I

Keynote

Developing an exemplary Security Culture at Swisscom: Change, Implementation and Success Factors

The need to implement an effective security culture change program is often triggered by societal, legal and technological innovation, e.g. social media, the blending of work and leisure, and mobile technologies. The initial step is to evaluate methodologies for measuring the current state and defining the new target state. If the project scope is clarified, the important program elements must be developed and implemented. Is a 'one-size-fits-all' approach reasonable, or do you have to choose a more role-based approach? How to be sure that the program runs effectively and gets the best possible acceptance? And how to evaluate progress during the success of your culture program?

The speaker will inspire with his experience and applied best practices a dialogue between peers.

Roundtable Session

Innovation in business, with cloud and mobility: How to measure, change and optimize security culture program

Change in technology means change in business, and this results in a changing culture. However, if the culture is not in focus, the culture will turn in any direction, not controlled by the company and its security function. First, the discussion is around change in technology and its consequences on security culture of people. How is a specific security culture assessed? How CISO can define new targets in culture and what is the difference to regular awareness. What is the relation to knowledge, attitude and behavior? And finally, which tools are in the CISO toolbox to turn around security culture, and in which case, which of the tools fits best.

The target of this discussion is to learn from each other about measuring, change-toolbox, and in which situations specific tools demonstrated good results.



Philippe Vuilleumier, Head of Group Security Swisscom AG, Master of Business Telecommunication, University Delft, has been with Swisscom since 2004.

Before being appointed as Head of Group Security (Chief Security Officer) in 2015, Philippe served in various roles in the network & IT Operations areas, his last position being the Head of Network & IT Operations. Before his time at Swisscom, Philippe held technical and management positions at Zurich Insurance Group, Equant and IBM. Twenty years' experience in several functions in the network and security domain gives him a large overview of different cultures, and in different countries as well. Recent big projects in the identification of security culture, transformation, and change are a solid foundation for the upcoming presentation at CISO Summit No 17. His view is associated with the telco & IT industry, and also relates to other companies, their needs, caveats and opportunities related to the security topic.

Session II

Keynote

Security Culture in SBB's Digitization Process: Analysis, Operational and Strategic Targets

Recent cyber security incidents indicate a fast-developing trend of indirect attacks on company through their vendors. Reason for that are improved proactive security measures and raising defense capabilities of many (larger) organizations and companies. Attackers, seeking to minimize effort to reach their attack targets, are increasingly targeting (smaller) third party service provider with lower defenses.

From there, they are moving laterally into their target organizations by misusing access credentials of these third-party service providers. Such attacks are often difficult to detect as they might show similar behavior patterns as normal cooperation. One measure to (partly) mitigate and minimize these risks is a systematic third-party information security monitoring. Scope is on watching trends and comparing targeted 3rd parties within their vertical.

To be effective, an interdisciplinary approach is needed, combining information security and ICT-security knowledge and experience with legal and procu-

rement capabilities because vendor management and a good contract and SLA basis are key to success. The presenter is currently discussing a joint approach to Third Party Information Security Management within the CISO community of SWITCH (CISOs of Swiss universities and research organizations) and will provide some insight on the targeted setup and value propositions.

Roundtable Session

Security Culture in Digitization Process: Analysis, Operational and Strategic Targets

Digitization in the railway system is very demanding as operational technologies need more consideration and analysis than just regular business IT. The discussion seeks to elucidate similar, recent or future experiences of participants with digitization. Top-down, elements of policies and strategies will be challenged. Agile digitization culture needs are reflected on personnel, operational technology and control system level; how to analyze the needs, how to identify gaps, and how to effectively change the culture.

During the roundtable session, the hypotheses as introduced during the keynote will be validated helping CIOs/CISOs to better identify cultural issues in digitization and operational technology, and the path to successfully perform a change program.



Jan Hohenauer, Deputy Chief Information Security Officer SBB AG, BSc and EMBA, University Fribourg, 2006 CISM certified.

He has 20 years' experience in Information Security: in consulting he was engaged with Identity & Access Management, PKI, Security Operations and Web-Security. In 2003 he joined SBB leading Network Security. Meanwhile, he founded the company-wide Center of Competence for Security. Later roles include strategic work for Telecom and Signaling departments. 2010 he joined the Information Security Team to lead the ICT-Risk Management and to enforce the integration of Operational Technology into the existing cybersecurity landscape, e.g. in Gotthard Base-Tunnel. From 2014 on-going he is the Deputy CISO and from January 2019 he acts as a "Product Owner" in a program strengthening SBB's Cyber Defence Capabilities.

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. This exclusive CISO Executive three ticket 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.

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



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
- 13:15 Welcome and introduction
- 13:30 Keynote from experts or members
- 14:20 Roundtable session I
- 15:20 Exchange between the groups and wrap-up of roundtable I
- 15:40 Break
- 16:00 Roundtable session II
- 16:50 Exchange between the groups and wrap-up of the roundtable II
- 17:10 Summary note
- 17:30 Cocktail and aperitif
- 18:00 Networking with VIP Party by Swiss Cyberstorm (optional)

The meeting is held three times per year.

Sponsorships

Platinum Sponsor

DETECON
CONSULTING

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

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

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.

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 17th 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

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 events, Summit 17 (15.10.2019), 18 (28.01.2020) and 19 (12.05.2020)

16th Swiss CISO Summit, October 15th, 2019 for CHF 450.– (single event)

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ Date _____

swisscisco summit

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

DETECON
CONSULTING



SWITCH



Sponsorships:

Platinum

Gold

Silver