Personal Invitation to 14th

swissciso summit

Next Generation Information Security Strategy: Impact, Data Governance & Implementation

30th October 2018 in Bern

DETECON CONSULTING

pwc

FUB | SWITCH

Sponsorships:

Platinum

Gold

Silver

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 14th 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

	Next Generation Information Security Strategy: Impact, Data Governance & Implementation
Date	**30th October 2018**
Time	**12:00 Lunch and 13:20 Summit: 8:30 h for those who like to enjoy Cyberstorm** (Networking with VIP party of Swiss Cyberstorm – Starting 18:00 Free Entrance offered by Swiss Cyberstorm)
Location	**Kursaal Bern** Kornhausstrasse 3, 3000 Bern, Schweiz
Keynote I	**Marcel Zumbühl, CISO Swiss Post Group and Lecturer ETHZ** Balancing between continuity and disruption: A review of effectiveness after 100 days in a new CISO position
Keynote II	**Stewart Kowalski, Professor Information Security, Norwegian Univesity of Science and Technology** Social Technical Strategy for Cyber Security and Risk
Key Benefits	• Experience industry best practices in the Swiss market • Actively participate 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 organisation

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

Summary

Next Generation Information Security Strategy: Impact, Data Governance & Implementation

For a long time it has been well-known and well-recognized that information security policies are the cheapest and most effective tool to increase security. However a proper strategy to reach the precious goals set in the policy is needed. This is where things start getting complicated in practice: The implementation of Information Security Strategies.

More often than not the term “Information Security Strategy” is defined circumstantially and thus does not possess a commonly agreed upon, well established meaning. It could represent the real implementation strategy of a security policy, but it is often used as an umbrella term for several high-level documents forming the foundation for information security governance in a company. In general, the Information Security Strategy needs to be well-tuned to the enterprise needs and socio-cultural ecosystem. If this is done successfully the implementation of and adherence to the strategy will fall into place smoothly. If the socio-cultural eco- system is not ready, a change program will help to prepare for the next steps.

The Information Security Strategy is a context related document, and must be different before the cloud, with the cloud, with anywhere / any time work and with massive IoT inclusion in to the company’s network. In addition, changes in society and new behavior of youngsters will challenge the CISO for having a buy-inn. To be successful in the long term, societal change needs to be modelled, understood and taken into account. Careful, early verification of the applied models can help to avoid obstacles and lengthy discussions.

At the 14th Swiss CISO Summit you will hear two leading speakers. One giving a retrospective on the experience of aligning the strategy during his first 100 days in his new position as CISO, and the other providing a research and innovation perspective which will give some essential background and introduce the round table discussions.

As usual, the goal of Summit 14 is to learn from the speakers, from each other and from the material distributed before the meeting for exploring today’s most recent tendencies in preparing, governing and implementing successfully high-level information security steering documents.

Session I

Keynote

Balancing between continuity and disruption: A review of effectiveness after 100 days in a new CISO position

Starting in a company is an adventure. Everything is new. In fact, you might be the only thing new in an otherwise stable and settled environment. But there is a reason why you are there, maybe the role is new, maybe the company has decided to move into another direction. A new CISO coming from outside the firm might be expected to review the security setting and the security strategy from a different angle, without jeopardizing the continuity of running processes There are expectations, some outspoken and some between the lines. The same goes for your new team and as every company has customers there are overarching customer expectations to explore. Starting fresh in a company is about expectation management, about carefully listening to outspoken and hidden expectations. About matching them with your experience and proposing a viable strategy and implementation plan that meets and exceeds expectations and matches the company's potential.

The security strategy of a company is part of the overall company strategy and needs to be endorsed by the board. IT should balance in internal and an external claim. What do you bring to your market clients and what do you bring to your company in terms of security? A vision can be a powerful tool to express what your company stands for in terms of security, it's inherent claim in the field. The security mission is how you see yourselves as a team, what is your purpose and what are the principles guiding you. What kind of security are you as CISO – the enabler or the enforcer?

Roundtable Session

Information Security Strategy Evolution and Change: How to analyze the as-is situation and measure effectiveness?

The Information Security Strategy (ISS) is one of the core documents in a corporation. Which context of the enterprise must be researched, vision, mission, general corporate strategy, value statement? Which methods work to quickly assess the strengths and weaknesses of an ISS? What is the scope by today, and what is the scope of the next period: What must be removed, what must be added? How to analyze the culture in an enterprise and how to use the result for well-tuned future development. How to decide, where to interact and correct or to let things run their course, when implementing an ISS. And what is the basic analysis for deciding when to act as an enabler and when to act as protector and reject solutions?

Marcel Zumbühl graduated as Master of Science at University of Bern in Computer Science and Business Administration.

He joined Swisscom Switzerland in 2002 and built-up the company's Security organization to effectively manage the whole security and safety portfolio encompassing cyber defence, business continuity and crisis management. In 2015 he changed industry to build and deliver the customer facing security of Credit Suisse's global digital private banking. He then became responsible for security steering of the digital global Compliance and Regulation Affairs. In summer 2018 he was appointed CISO of the Swiss Post Group and joined the IT Board Marcel Zumbühl lectures in risk management and risk communication since 2009 and is frequently leading workshops at conferences both internationally and in Switzerland on Security, Privacy and Trust.

Session II

Keynote

Soco-Technical Strategy for Cyber Security and Risk?

Learning how simple models can be used to deal with the complex cyber security threats your organization is facing today and in the future.

The need to manage security and risk in organizations is not new. However, every day newspaper headlines are filled with reports about new growing cyber security threats. Headlines of million dollar frauds and leaks of international corporate secrets appear at least once a week. Neither organization nor nation – no matter how large – seems to be able to defend themselves from such attacks. Are all secure management systems fundamentally insecure in todays cyber world and must we just learn to live with insecurity?

To answer this question, we need to review some of the fundamental principle of socio-technical systems design and risk management. In this lecture simple some socio-technical models and techniques will be introduced and examples of how these models can be used to measure and communicate cyber security risk in your organization will be illustrated.

Roundtable Session

Socio-Technical models & analysis: What is it's value proposition and how to successfully apply these models?

Are the security models we us today good enough to measure and manage the complex risk organizations face in the cyber world? What value can new socio-technical models bring to the table? Can a socio-technical model help both to find the secuirty gaps and also fill them? Are some organization more mature to hand societal and technological changes than others? Can socio-techincal maturity really be measured in practise?

A socio-technical framework used to model and measure security incident handling will be presented to the roundtables. Roundtable delegates will than discuss and rank the socio-technical risk escalation mature of different organizations by reviewing documented responses of these organization to common security events. Each table will try and reach an consensus on the ranking of the maturity of the different organizations. These ranking will than be discussed and debated between the tables. Can new models helps us to understand identify and communicate common security problems and agree on appropiate security solutions. Or do new models only create new names for old problems?

Professor Stewart Kowalski: Has both extensive industrial and academic experience in information security, security education and awareness training. He hasworked on education and awareness issues in security as risk and security manager for Ericsson Global Services and as Chief Security Architect for Huawei technologies. He has worked in a number of European Research Projects and has published over 100 articles in the field of information security during the last 30 years.

He is currently professor of Information Security at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology. He is also the current head of the Information Security Management Group at the Centre for Cyber and Information Security, CCIS, www.ccis.no and Program Director for 3 Master Programs in Information security.

Registration

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to max. 40 per summit for maintaining 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)

Cancellation Policy
Cancellations of registration are free of charge but 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, however, 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.

□ **Three consecutive summits for CHF 1'000**
3 events, Summit 14 (30th October 2018), 15 (29th January 2019) and 16 (21st May 2019)

□ **14th Swiss CISO Summit,** 30th October 2018 **for CHF 450.– (single event)**

First Name ______________________ Surname ______________________

Organisation ____

Street / No. ______________________ ZIP / City ______________________

Phone ______________________ Email ______________________

Signature ______________________________ *Date* ______________

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. The summits are held strictly under the Chatham House Rules, which is the ruleset to treat the shared information with full discretion.

- 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 the current strategies on managing security threats today and to prepare for the future
- Make new connections and equip yourself with insider 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 today’s 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 today is the Head of the new BSc Information & Cyber Security at Hochschule Luzern / Informatik. Additionally, he also teaches at the Norwegian University of Science and Technology 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**

DETECON
CONSULTING

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**

pwc

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**

SWITCH

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)

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.