Personal Invitation to 15th

swissciso summit

CMMI & Risk Management

Methodology advancement, business impact & resilience improvement

29th January 2019 in Zurich

DETECON CONSULTING

pwc

FUB

SWITCH

Sponsorships:

Platinum

Gold

Silver

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 15th 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

	CMMI & Risk Management **Methodology advancement, business impact & resilience improvement**
Date	**29th January 2019**
Time	**12:00 Lunch and 13:00 Summit**
Location	**Zunfthaus zur Schmiden** 1. Stock, Marktgasse 20, 8001 Zürich, Schweiz
Keynote I	**Effective Cyber Defense in Industry 4.0** Andy Mühlheim, Head of Division Information Technology, Endress+Hauser Flowtec AG
Keynote II	**CMMI Cybermaturity Platform: An experience report of an early adopter.** Ivo Maritz, CISO BKW
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

CMMI & Risk Management: Methodology advancement, business impact and resilience improvement

The ever-pending questions for those who invest into information and cyber security are: Are we under-invested, i.e. at risk to be below due diligence, are we overinvested, i.e. we are wasting money, and are our measures the best possible set for the given invested money in respect to effectiveness and efficiency?

The answer of these questions is provided by risk management, sector wise sharing circles for identifying the position in the sector, and the study of most common frameworks to double check the completeness of security risk measures. The time of the security office is always short, and therefore the best strategies to identify risks and to create the best possible set of measures is desired. Against this context, two major approaches are available: the risk based approaches like ISO 27 001 / NIST / BSI base line protection manual and the CMMI model, which relates to controls. For each control are levels defined (Initial, Managed, Defined, Quantitively Managed, Optimizing), which show precisely, how advanced the control is implemented and how deeply integrated in the security processes.

At the 15th Swiss CISO Summit you will hear two leading speakers, both well-known to our community and with in-depth experience in information and cyber security: One giving the experience of risk analysis and risk management, considering the corporate need, and the social needs, and the other providing initial experience with the new CMMI cyber resilience framework, positioning CMMI against other well-known risk-based frameworks. Both speakers prepare the ground for the following discussion and introduce the round table discussions.

As usual, the goal of Summit 15 is to learn from the speakers, from each other and from the material distributed before the meeting for exploring today's most recent trends in addressing the information and cyber security challenge with the best set of controls.

Session I

Keynote

Effective Cyber Defense in Industry 4.0

Traditional Cyber Defense is obsolete in the context of Industry 4.0 or to put it in an even more blunt way: cyber security in the form as we know it today is dead. When conducting digital business traditional cyber security is considered a hygiene factor. To plan and implement efficient cyber security as needed we need to understand global trends and their convergence. Technology, economy, society, politics and conflicts between nation states and the assessment of these factors will ultimately decide on strategy and measures a company might implement to address cyber related risks. Core business functions are requesting to support new business models as e.g. cloud-based models bringing new requirements for security into the organization's security plan.

Whilst addressing new requirements from a security perspective the CIO/CISO faces the challenge of balancing risks and measures. Potentially security over-investments will limit the flexibility in implementing new business models and ultimately will lead resistance against cyber security measures from core business functions teams.

Roundtable Session

Cyber Defense in Industry 4.0 in action – best practice sharing

Planning, developing and implementing a consistent Information Management architecture will help in reducing the exposure to potential threats. The CIO/CISO is expected to focus on the mid layer of the risk pyramid when conducting a risk assessment and defining measures as the base needs to be covered anyway irrespective of risk profile and risk appetite. Core business functions will find (cloud based) solutions to support their digital business giving rise to potentially new shadow-IT neglecting security related aspects. By taking a proactive role and having the self-conception of being the sparring partner and facilitator to core business functions the CIO/CISO will add immense value to both business and cyber security.

During the roundtable session the hypotheses as introduced during the keynote will be validated helping CIOs/CISOs to better fulfill business requirements be that from an architecture, infrastructure or data driven standpoint

Andy Mühlheim holds a BSc in Electrical Engineering, a BSc in Industrial Engineering and a MBA (SUNY). He holds the rank of a Major in the Swiss Armed Forces (Cyber Defense) and is listed as expert for cyber security of the Swiss Academy of Engineering Sciences.

Andy has 20 years of leadership experience in mid and large sized organizations, including CIO and CSO of a national critical infrastructure. He is an expert for digital transformation, critical systems protection and cyber defense. He is an experienced leader with broad skills in the IT, telecom, energy and manufacturing industry. He is a member of the expert group cyber defense of the department of defense.

Since August 2017 Andy Mühlheim is the Head of the IT Division of Flowtec, an Endress+Hauser subsidiary, with manufacturing sites in CH, FR, CN, US, IN and BR. He has been assigned with Flowtec's digital transformation and the IT/OT convergence.

Session II

Keynote

CMMI Cybermaturity Platform: An Experience Report of an Early Adopter

This past April 2018, the CMMI Institute, well known for over 25 years for its Maturity Model, has launched the CMMI Cybermaturity Platform; a SaaS-Application based on a comprehensive method for a risk-based assessment of an organization's cybersecurity capabilities with regard to its people, processes and technologies.

The presenter had the opportunity to accompany the development of the CMMI cybersecurity capability assessment application throughout 2017 and to run a beta evaluation with BKW as a corporation and with seven of its business units (BUs) in early 2018. He will report on his experiences with assessing the cybersecurity risks for BKW, getting the required target cybermaturity level to cope with these risks, measuring the actual maturity levels of BKW and its seven BUs, comparing them with initially determined target, working with the roadmaps to close the gaps.

He will also show how he compiled the target and the actual cybermaturity levels to compare them with the objectives of the BKW Cyber Security Program on one side and with the new NIST Cyber Security Framework that corresponds to the new Swiss IKT Minimalstandard on the other hand. These build the foundation for the upcoming report to the Executive Committee and the Board of Directors of BKW AG.

Roundtable Session

CMMI cybersecurity capability assessment: What is the scope of CMMI? What is new and in which aspects is CMMI cybersecurity capability assessment different from traditional methods. Does CMMI make life of the CISO easier or even more complicated? Which is the gain for the CISO and for the CEO, e.g. in respect to the clarity of alignment with the business goals.

What is important when starting with the new concept, either in some controls only or with the full set of questions? Is CMMI cybersecurity capability assessment for all industries equally important or can we identify differences with the various industries? Are specific expectations how regulators will react on the new framework? Is there any shift of the due diligence duties expected in near future? Is CMMI cybersecurity capability assessment times saving or time consuming?

Ivo Maritz works for BKW since March 2014. He led the ICT as the Group CIO and Head of the ICT Business Unit until the end of 2016 and heads Cyber Security as the CSO/CISO since January 2017. In both functions he reported and reports to the CFO and Member of the Group Management. Currently Ivo Maritz focuses on the implementation of the group wide Cyber Security Program. To that goal, he runs five streams addressing Governance, Awareness, IT & OT Protection, Resilience & Recovery as well as Operation Initialization with 25 individual projects over 3 years. Before joining BKW Ivo Maritz led ICT organizations with a global Pharmaceutical, a Swiss Tele¬communications and a global Machinery Corporation for more than 25 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 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 15th 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 events, Summit 15 (29. 01. 2019), 16 (21. 05. 2019) and 17 (15.10.2019)

☐ **15th Swiss CISO Summit, January 29, 2019 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

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.