

Risk Center Continuing Education

# Cyber Risk

How to Navigate through the Digital  
Transformation

Block Course in Fall 2019



# Cyber Risk: How to Navigate Through the Digital Transformation

## About the Course

As today's technology landscape is evolving at an increasing pace, it forces businesses, individuals and society to adapt to stay competitive. At the same time, the risk to businesses from cyber-attacks is growing just as fast, if not faster. Staying on top of today's cyber risks means understanding the key drivers of cyber risk and remaining aware of the latest trends, research, solutions and best practices.

This course offers an integrative perspective on cyber risks, allowing understanding the essential developments, the principles, the challenges as well as the limitations and the state of practice in cyber risk from the technological, economic, legal, and insurance perspective. It focuses on tangible takeaways that cyber risk stakeholders in all organizations can use to strengthen their resilience.

The course provides an interdisciplinary overview, guidance, and understanding of the mechanisms in cyber security to guide decision making and risk management in business and society.

## Contents

### From Fortress to Resilience

Resilience is based on the premise that protective, preventive, and deterrent safeguards will not always be effective (i.e. successful in

keeping out a threat) and therefore will require response, recovery, and restorative action

### Technical Fundamentals of Information Security

This part will cover examples of today's challenges and problems related to information security from a more technical point of view. We look at a set of principles/guidelines to build secure systems. In the second part we look at examples of cryptographic primitives that provide the building blocks for many security critical applications. The goal is to give an impression of the technical side of information security and the challenge of providing provably secure and trustworthy fundamentals (algorithms, protocols).

### Key Drivers, Supply Chain Security and Internet of Things

In connecting people and machines ever more closely together, the Internet has changed our lives forever in just two decades. These changes are disruptive, like the introduction of electricity, railroads, or airplanes. This latest digital innovation is not the first to prompt critical questions regarding security and safety. New possibilities as well as threats emerge at the interfaces of technology, economy and society. What are the cyber threats and defenses for society and the industry in the digital age? What are the lessons we can draw from other industries or history?

## Who should attend?

The course is designed to appeal to a wide audience of decision makers and to provide actionable information for all professionals that play a role in managing cyber risk in their organization—not just IT professionals. Participants will work and exchange, in small groups, with some of the best researchers, experts, and practitioners working at the cutting edge of their discipline, and among peers. It allows communicating risks and solutions in terms that will resonate with corporate and institutional stakeholders.

## Cyber Insurance

As IT security practitioners are becoming more and more pessimistic than in past years about their ability to protect their organizations from cyber security threats, yet, despite this apparent increase in the frequency and severity of cyber losses, the cyber insurance market has continued to grow and evolve. However, thus far actuaries have approached cyber risk with caution. In these two sessions, cyber risk experts will share their insights on the state of the cyber insurance market and the evolution of underwriting cyber risk, including information about the limitations of cyber insurance

## Critical Infrastructures: Energy System

In a digitized world, the resilience of the energy system must be reunderstood: On the one hand, digitization offers opportunities for greater resilience, on the other hand, vulnerability can increase. This is all the more difficult because the energy system itself is already expecting disruptive developments. In particular, minimizing the risk of a major blackouts is of the utmost importance. How can this be achieved? In the lecture the following will be presented:

- What makes the critical infrastructures (CIS) energy so special?
- What are the basic principles of a resilient CIS system design?
- How are digitization trends changing energy supply?
- What are the root sources for the new risks?
- What are some technical, organizational and regulatory measures with which these risks can be countered?
- Who determines the risk appetite of a nationally critical infrastructure

## Critical Infrastructures: Financial Institutions

Financial institutions, as they maintain the most mature cyber security programs, have moved beyond the "predict and protect" paradigm to a concept of cyber resilience in order to face

the broad range of interdependent disruptive hazards. In addition, the digital assets are also under constant attack by cyber criminals all around the world. This combination of unprecedented level of attacks has a very significant impact on the most robust organisations. This part will unpack these challenges and response methodologies, covering also cognitive and social dimensions as an integral part of cyber resilience.

## Final Panel Discussion on Governance

An organisation's board is responsible for the framework of standards, processes and activities that, together, secure the organisation, also against cyber risk. This course will close with a panel discussion on how to cope with the cyber threat landscape from a governance perspective.



## Structure

The course is structured as 10 Evening Sessions (18:00 to 20:00) on Thursdays with a networking apero after each session.

### Part 1: What is Cyber Risk Management?

24 Oct 2019

31 Oct 2019

### Part 2: Theoretical Foundations of Cyber Security

7 Nov 2019

14 Nov 2019

### Part 3: Managing Cyber Risks, Actors and Threats

21 Nov 2019

28 Nov 2019

### Part 4: How to Model and Mitigate Cyber Risk

5 Dec 2019

12 Dec 2019

### Part 5: Cyber Risk and Critical Infrastructures

9 Jan 2020

Visit to UBS  
(tba)

### Part 6: Concluding and Panel Discussion

16 Jan 2020

## Language

The course language is English

## Number of Participants

The number of participants is limited to 30.

## Course Fee and Registration

CHF 2 500.-

Registration deadline is October 11, 2019

## Certificate

Participants get a certificate for confirmation of participation.

## Venue

ETH Main Building  
Rämistrasse 101

## Lecturers (ETH)

**Prof. Dr. Paul Embrechts (Course Director)**

Risk Center and RiskLab (D-MATH)

**Dr. Stefan Frei**

Lecturer Cyber Security D-MTEC, Cyber Security Principal, Accenture Cyber Defense

**Prof. Hans Rudolf Heinimann**

Past Director, Future Resilient Systems, ETH Singapore Center

**Dr. Patrick Schaller**

Lecturer and Coordinator CAS in Cyber Security, D-INFK

**Dr. Spencer Wheatley**

Chair of Entrepreneurial Risk, D-MTEC

**Prof. Dr Martin Wörter**

KOF Swiss Economic Institute, D-MTEC

## Lecturers

**Prof. Dr. Marie Kratz**

ESSEC Business School, Paris

**Reto Amsler**

ALSEC Cyber Security Consulting AG

**Anne Bouverot, Anne B Advisors**

Chair Panel Session on "Governance"

**Dr. Michel Dacorogna**

Partner by Prime Re Solutions, Zug, Switzerland

**Michael Dargan, Group CIO, UBS**

**Neal Pollard, Group CISO, UBS**

on "Managing Cyber Risk: A View From a Bank"

**Roger Halbheer, Chief Security Advisor, Microsoft EMEA**

on "Cloud is a Security Imperative?"

**Prof. Dr. Marie Kratz**

ESSEC Business School, Paris

**Christoph Mayer**

OFFIS, Institute for Information Technology, Germany

**Marc Ruef**

Security Expert, scip AG,

on "Darknet - A Look at the Digital Underground"

## Coordination and Contact

**Dr. Bastian Bergmann**

Executive Director, ETH Risk Center

bbergmann@ethz.ch

## **Contact**

ETH Zurich  
Risk Center  
Scheuchzerstrasse 7  
8092 Zurich  
Switzerland

[www.riskcenter.ethz.ch](http://www.riskcenter.ethz.ch)  
[info-riskcenter@ethz.ch](mailto:info-riskcenter@ethz.ch)