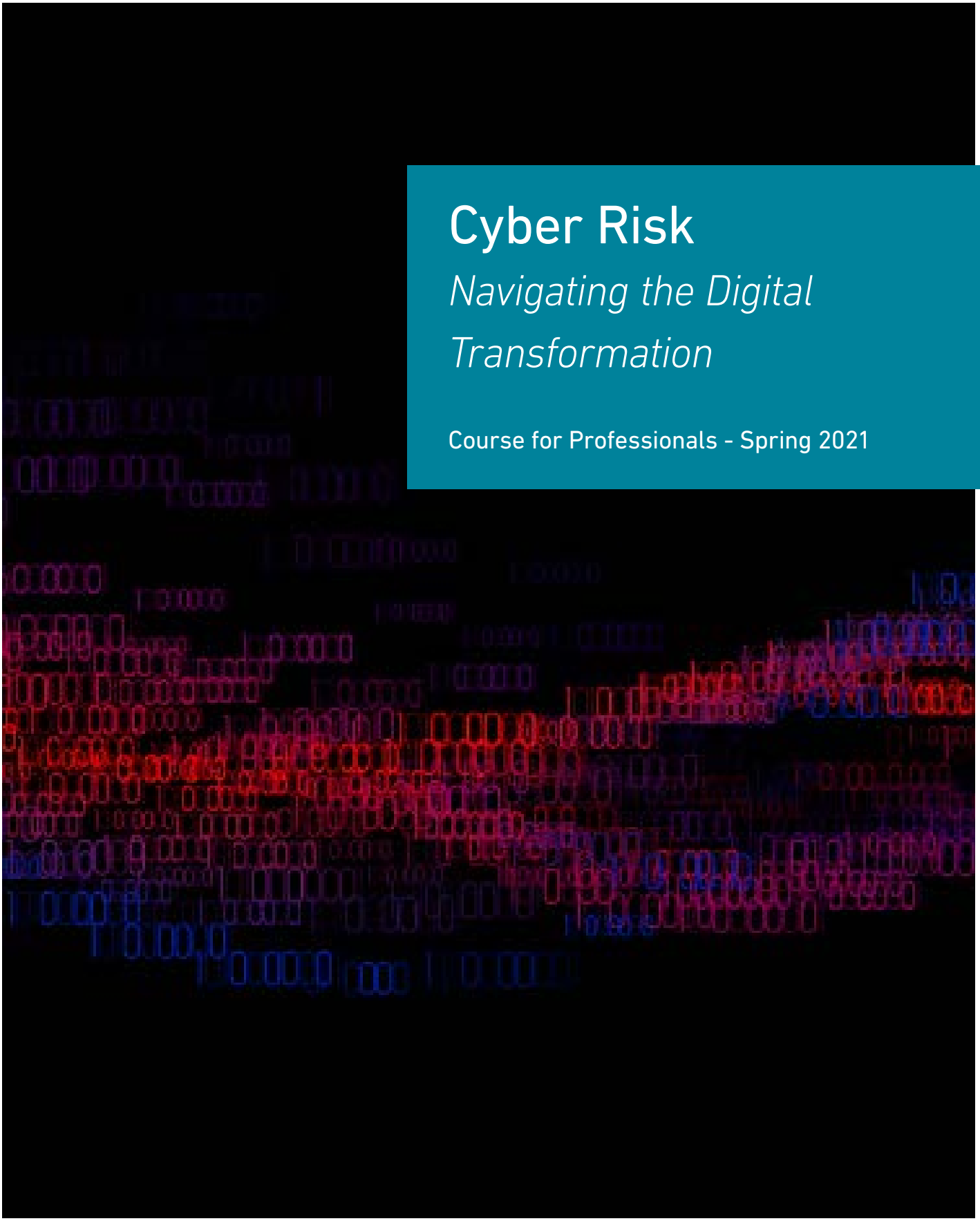
ETH zürich



Cyber Risk

Navigating the Digital Transformation

Course for Professionals - Spring 2021

ETH RISK CENTER

Cyber Risk: How to Navigate the Digital Transformation?

The technology landscape is evolving at an increasing pace, forcing businesses, individuals and society to adapt in order to remain competitive. At the same time, the risk of cyber attacks on businesses is growing just as fast, if not faster. To keep on top of such risks, one must understand the key drivers of cyber risk and get updates on the latest trends, research, solutions and best practices.

Who should attend?
The course is designed to appeal to a wide audience of decision-makers and to provide actionable information for all professionals playing a role in the management of 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. They will learn to communicate about risks and solutions in terms that will resonate with corporate and institutional stakeholders.

Course coordinator
Dr. Christian Waibel
ETH Risk Center
cwaibel@ethz.ch

Practical Details

About the Course
This course offers an integrative perspective on cyber risks. It helps understand the important developments, the principles, the challenges and limitations, and the state of practice surrounding cyber-risk from the technological, economic, legal, and insurance perspective. The course provides tangible takeaways that cyber risk stakeholders in all organizations can use to strengthen their resilience.

Participants gain an interdisciplinary overview and an understanding of cybersecurity mechanisms, which will guide their decision-making and risk management.

Language
English.

Number of Participants
Limited to 30.

Fee and Registration
CHF 2,000.-
Registration deadline: 01.04.2021

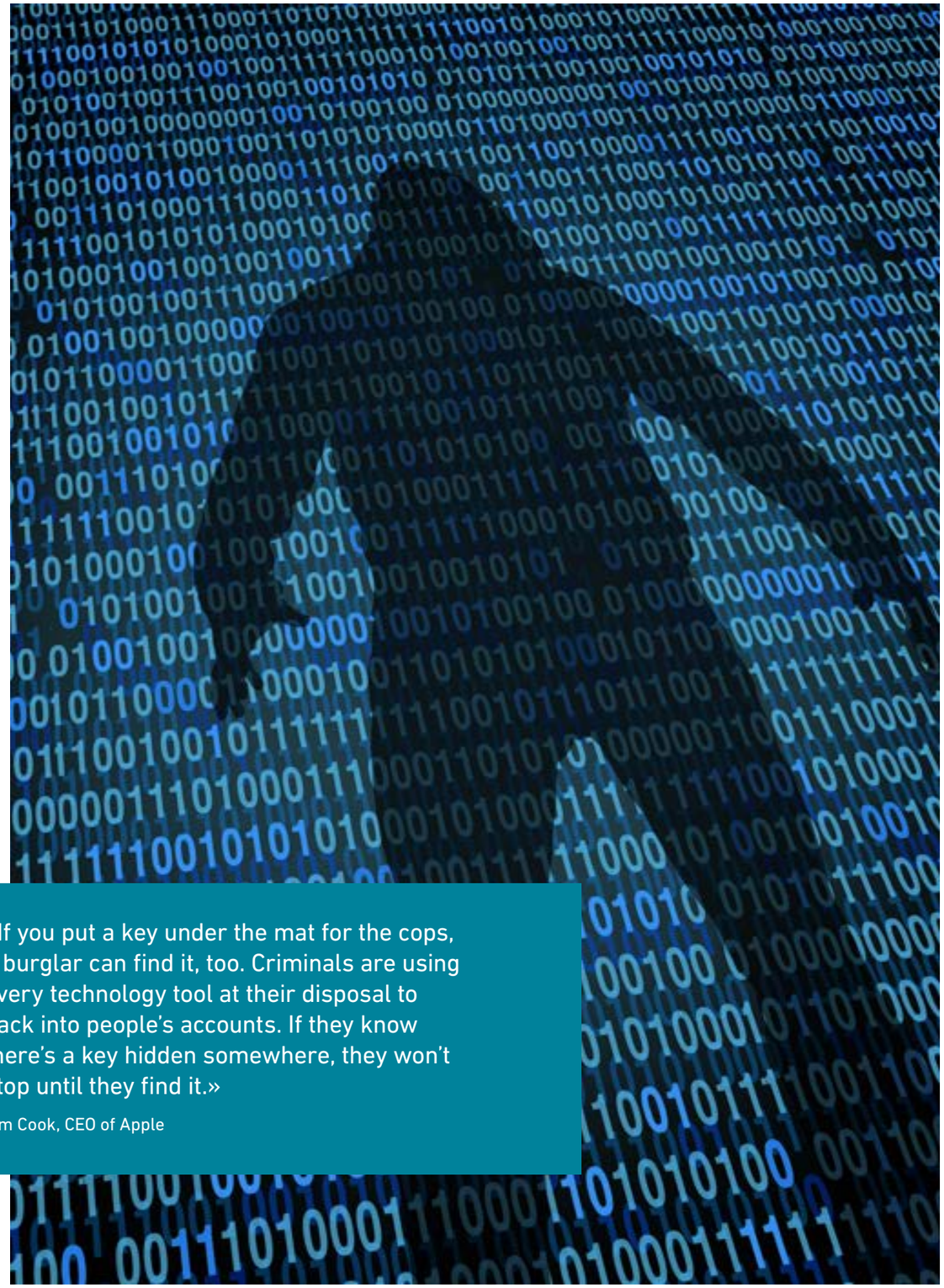
Certificate
Participants get a certificate for confirmation of participation.

Venue: Virtual and Classroom at ETH Zürich
Given the current uncertainty about the Covid19-related restrictions, the course is set up as a hybrid of online sessions and physical session for discussion and networking at ETH Zürich.

Structure

The course comprises 7 parts. Each part is divided into 1 to 3 sessions, mostly on Thursdays from April to July (from 18:00 to 20:00). The course also includes a Public Session, open to the Risk Center's community of professionals. It will engage the course's participants in a larger dialogue around the topic of cyber risk.

Sessions 1+2	Managing Cyber Risk, Threats, and Actors
Sessions 3+4	Theoretical Foundations of Cyber Security
Sessions 5+6	Cyber Resilience and System Architectures
Sessions 7-9	How to Model and Mitigate Cyber Risk?
Public Session	Cyber Risks in Critical Infrastructure & Health Care Markets (1 full day)
Session 10	Critical Infrastructre Protection
Session 11	Cyber Risk Governance



«If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it.»

Tim Cook, CEO of Apple

Course Contents: From Fortress to Resilience

Resilience is based on the premise that protective, preventive, and deterrent safeguards will not always be effective. Therefore, potential threats 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 perspective. We look at a set of principles/guidelines to build secure systems and look at examples of cryptographic primitives that provide the building blocks for many security-critical applications.

Cyber Resilience and System Architectures
The integration of large IT systems to their functions and scope has become critical to any organization. The notion that integration offers easier and safer control over the whole range of operations does not always hold. Security measures require an increased effort to keep up with the complex IT systems implemented across all the organization's scope. Maintenance procedures are now done autonomously and have to continuously be updated to address problems and efficiency measures referring to various assets and operations.

How to Model and Mitigate Cyber Risk
As IT security practitioners are becoming more pessimistic than in past years about their ability to protect their organizations from cybersecurity threats, 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 cyber insurance market's state and the evolution of underwriting cyber risk, including information about the limitations of cyber insurance.

Critical Infrastructure
This digital innovation is not the first to prompt critical questions regarding security and safety. These attacks are disruptive, as the introduction of electricity, railroads, or airplanes. Yet, there's no such thing as a "random" attack. 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?

Health Care Markets
Healthcare makes up 12% of the GDP in Switzerland. Health data is among the most private. Healthcare providers have access to patient data and can add information. These include data of diagnosis as well as treatments. Cyber risks do not stop at doctors' doors. The NHS estimated the costs of the Wanna Cry attack, in which 19,000 appointments were canceled, at 92 million pounds. Estimates suggest that health data is worth more than ten times the same amount of data about purchases. What kind of information is critical? What kind of critical data is at risk in hospitals? What risks are most likely to realize for health providers?

Critical Infrastructure Protection
In a digitized world, the energy system's resilience must be reunderstood: On the one hand, digitization offers opportunities for greater resilience. On the other hand, the 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 major blackouts is of the utmost importance. How can this be achieved? What are the root sources for the new risks? What are some technical, organizational, and regulatory measures with which these risks can be countered?

Cyber Risk Governance and Organisation
An organization's board is responsible for the framework of standards, processes, and activities that, together, secure the organization, also against cyber risk. Is there a legal obligation for compliance assessments? Does a duty to act arise from the "findings"? Moreover, finally, what are the legal requirements for actors?

The topics of Critical Infrastructure and Health Care Markets will be discussed during a Public Session.

«Thinking of cybersecurity solely as an IT issue is like believing that a company's entire workforce, from the CEO down, is just one big HR issue.»

Steven Chabinsky, Global Chair of Data, Privacy & Cybersecurity at White & Case LLP

Speakers and Dates

Lecturers:

ETH
Prof. Paul Embrechts
Risk Center and RiskLab, D-MATH
Stefan Frei
Lecturer Cyber Security D-MTEC, Senior Information Security Officer, SIX Digital Exchange SDX
Prof. Kenneth Paterson
Applied Cryptography Group, D-INFK
Prof. Adrian Perrig
Network Security Group, D-INFK
Patrick Schaller
Senior Scientist, Cyber Security Group, D-INFK

External
Erik Dinkel
Chief Information Security Officer, UniversitätsSpital Zürich
Prof. Michel Dacorogna
Partner, PRS Prime Re Solutions
Noel Ferguson
Managing Director Global Technology, UBS
Roger Halbheer,
Chief Security Advisor, Microsoft EMEA
Prof. Hannes Lubich
Fachhochschule Nordwestschweiz
Klaus Julich
Managing Partner, Deloitte
Prof. Marie Kratz
École Supérieure des Sciences Économiques et Commerciales
Ivo Maritz
Senior Advisor, Monti Stampa Furrer
Franco Monti
Partner, Monti Stampa Furrer
Neal Pollard
Chief Information Security Officer, UBS AG
Maxim Salomon
Technical Program Manager for Security of Mergers & Acquisitions, Google
Andreas Schönenberger
Chief Executive Office, Sanitas Group
Iwan Stalder
Head of Group Accumulation Management, Zurich Insurance
David Wicki-Birchler
Board Member, LEANmade

Dates and times:

Session 1:	April 8	6pm to 8pm	online via Zoom
Session 2:	April 15	6pm to 8pm	online via Zoom
Session 3:	April 29	6pm to 8pm	online via Zoom
Session 4:	May 6	6pm to 8pm	tba
Session 5:	May 20	6pm to 8pm	tba
Session 6:	May 27	6pm to 8pm	tba
Session 7:	June 10	6pm to 8pm	tba
Session 8+9:	June 18	3pm to 7pm	tba
Public Session:	June 24	Full day	tba
Session 10:	July 1	6pm to 8 pm	tba
Session 11:	July 8	6pm to 8pm	tba

Impressions of Past Participants

"The course format is excellent for professional education."

"Very varied and balanced selection of topics"

"Very interesting, much information, sometimes the technical aspects are too detailed. But appropriate for a course at ETH."

ETH Zürich
Risk Center
Scheuchzerstrasse
8092 Zürich

www.riskcenter.ethz.ch
info-riskcenter@ethz.ch