CAS Cyber Risk & Security HWZ

Digitalisierung ist eine globale Revolution. Sie verändert Geschäftsprozesse, bedroht langjährige Geschäftsmodelle und prägt die Art und Weise, wie Innovationen in Unternehmen begegnet wird. Die digitale Transformation führt aber auch zu neuen Risikofaktoren, die weit über die typischen Bedrohungen von traditionellen IT-Systemen hinausgehen.

Cyber Risk & Security bildet eine Brücke zwischen der Geschäftsstrategie, technischen und betrieblichen Aspekten sowie der Unternehmenskultur. Das Ziel ist, digitale Gefährdungen neu aus einer ganzheitlichen, unternehmerischen Perspektive zu beurteilen und mit geeigneten Massnahmen die Widerstandsfähigkeit (Digital Resilience) des Unternehmens im digitalen Geschäft zu erhöhen.

It's Business, not Bytes

Der CAS Cyber Risk & Security fokussiert auf Risiken in den Bereichen Infrastruktur und Reputation sowie im Bereich der Märkte und Geschäftsmodelle, die spezifisch im Zusammenhang mit der Digitalisierung zu adressieren sind. Dozierende aus der Privatwirtschaft und aus Behörden verschaffen Ihnen detaillierte Einblicke in die aktuelle Bedrohungslage für die Schweizer Wirtschaft.

Der CAS beschäftigt sich mit Themen wie Cybersecurity, Hacking, Data Privacy oder Krisenkommunikation. Ausserdem werden die Teilnehmenden in die Grundlagen verschiedener Risk Management Frameworks und internationaler Standards eingeführt.

Der CAS Cyber Risk & Security ist ein in sich geschlossener Zertifikatslehrgang mit Leistungsnachweis. Studierenden mit MAS-Zulassung kann er als Wahlmodul an den MAS Digital Business angerechnet werden.

Ihr Nutzen

- Anrechnung an den MAS Digital Business der HWZ
- Hacking Lab
- Hands-on-Workshops
- Impulsreferate

Facts & Figures

Abschluss
«Certificate of Advanced Studies (CAS) in Cyber Risk & Security»

Anerkennung
15 ECTS-Kreditpunkte

Pensum
Berufsbegleitender Studiengang. 100-prozentige Arbeitstätigkeit möglich.

Beginn
Studienbeginn ist jeweils im Februar. Die Studiendaten finden Sie auf der Website.

Dauer
1 Semester (18 Tage)

Anzahl Teilnehmende
Die Studiengruppe umfasst maximal 24 Personen.

Studienort
Das Studium findet im Gebäude «Sihlhof» im Herzen von Zürich statt. Der «Sihlhof» befindet sich direkt beim Hauptbahnhof, im trendigen Stadtteil der Europaallee.

Studiengebühren
Die aktuellen Studiengebühren finden Sie auf der Website.

Blog
www.hwzdigital.ch

Website
www.fh-hwz.ch/cascrs

CAS Cyber Risk & Security HWZ

Digitalen Gefahren weitsichtig begegnen und Chancen der Digitalisierung nutzen

Ziele und Perspektiven

Das Verstehen von Digital Risk Management als Geschäftsleitungsaufgabe, das Beurteilen digitaler Gefährdungen aus einer ganzheitlichen unternehmerischen Perspektive und das Identifizieren von Chancen der Digitalisierung stehen im Zentrum des Studiengangs. Konkret heisst das:

- Sie nutzen die sich daraus ergebenden Möglichkeiten für Ihr Unternehmen.
- Sie kennen die aktuelle Bedrohungslage von Unternehmen und Mitarbeitenden im Bereich Cybercrime und können diese einordnen.
- Sie können die häufigsten Angriffsarten und deren mögliche Auswirkungen auf den Betrieb identifizieren.
- Sie sind mit den Pflichten des Datenschutzes und insbesondere den neuen EU-Regulationen und deren Auswirkungen auf die Geschäftsprozesse vertraut.
- Sie können die Chancen und Risiken disruptiver Geschäftsmodelle aufzeigen.
- Sie kennen die rechtlichen Aspekte von Big Data.
- Sie sind mit verschiedenen Standards und Risk Management Frameworks und deren Positionierung vertraut.
- Sie kennen die Grundlagen für die Organisation einer Krisenkommunikation.
- Sie können eine geeignete Digital Risk Management Governance konzipieren und kennen die entsprechenden Organisationen in der Schweiz.
- Sie können das Management und die Mitarbeitenden für das Thema Digital Risk Management sensibilisieren.

Teilnehmende

Der CAS Cyber Risk & Security richtet sich an Entscheidungsträger, Fachkräfte mit direkter Verantwortung oder indirekten Bezügen zum Management von digitalen Geschäftsfeldern: Profis im Produktmanagement, in der Informatik, in der Kommunikation, E-Business-Verantwortliche, Risk Manager und Security Officers.

Es sind keine spezifischen IT-Vorkenntnisse nötig.

Zulassung

Zugelassen werden Personen mit einem Hochschulabschluss oder äquivalenten Abschluss und mindestens zwei Jahren Berufserfahrung.

Personen mit anderen Bildungsabschlüssen wie zum Beispiel TS, HF und höheren Fachprüfungen mit eidg. Abschluss können «sur dossier» aufgenommen werden.

Aufbau und Inhalt des Studiengangs

Der Lehrgang fokussiert auf Risiken mit spezifischem Bezug zur Digitalisierung. Er ist nicht als klassische Risk-Management-Ausbildung positioniert, sondern adressiert explizit auch die Chancen, die sich im Rahmen von digitalen Geschäftsmodellen ergeben.

Interdisziplinär und integral

Der Kurs startet mit einer Einführung ins Digital Risk Management, in die Digitalisierung sowie die Informationssicherheit.

Der Schwerpunkt liegt bei den digitalen Risikotreibern, allen voran Cybercrime und Cyberwarfare, aber auch bei den Risiken disruptiver Geschäftsmodelle und zunehmender Regulationen im Bereich des Datenschutzes und der Datenverarbeitung.

Die aktuellen Gefahren für Unternehmen werden porträtiert und die verschiedenen Angriffsarten detailliert und verständlich erörtert. Im Kontext des Hacking Lab können die Teilnehmenden danach mit echten Hacking Tools selbst Hand anlegen. Der Lehrgang ist aber nicht nur technisch orientiert. Der Umgang mit digitalen Reputationsrisiken, rechtlichen Aspekten von Big Data und der Absicherung von neuen, digitalen Geschäftsmodellen gehört genauso dazu wie der Umgang mit Risiken in agilen Entwicklungsmethoden und die Positionierung als attraktiver Arbeitgeber für Digital Natives.

Für die Implementation einer Digital Risk Management Governance werden verschiedene Standards und Risk Management Frameworks miteinander verglichen, aber auch die Sensibilisierung von Mitarbeitenden und vom Management werden thematisiert.

Praktische Hands-on-Workshops, ein Hacking Lab, eine Exkursion sowie Impulsreferate runden den Präsenzunterricht in den HWZ-Räumlichkeiten ab.

Schlüsselinhalte

- Cybersecurity
- Hacking
- Social Engineering
- Data Privacy
- Shitstorms & Reputation Campaigners
- Personal Reputation Management
- Risk Insurance

Ihre Experten

Sie und die Studiengruppe

Mit Ihren bisherigen Kompetenzen und Fähigkeiten aus Aus- und Weiterbildung sowie aus Ihrer beruflichen Tätigkeit sind auch Sie und alle anderen Studiengruppenmitglieder Expertinnen und Experten auf einem bestimmten Gebiet. In einer spannenden, heterogen zusammengestellten Studiengruppe profitieren alle voneinander, indem alle ihr Wissen und ihre Erfahrung aktiv einbringen, teilen und erweitern können.

Dozierende

Der Kreis der Dozierenden rekrutiert sich aus Vertretern von führenden Markenartiklern, Marketing-, Werbe-, PR- und Online-Agenturen, Unternehmens- und Kommunikationsberatern sowie Hochschuldozierenden mit reicher Praxiserfahrung und hohem Praxisbezug.

Zu den Dozierenden gehören unter anderen:

Ferdinand Kobelt
Chief Security Officer,
Swiss Federal Department of Defence,
Civil Protection and Sport

Ivan Bütler
CEO, Compass Security

Thomas Bögli
Chef Cyber-Defence der Schweizer Armee

Bruno Baeriswyl
Datenschutzexperte, ehem.
Datenschutzbeauftragter, Kt. Zürich

Matthias Bossardt
Head Cyber Security Services, KPMG

Tobias Bolliger
Senior Cyber Advisor at
Swiss Federal Office of Police fedpol

Institute for Digital Business

Das Institut realisiert massgeschneiderte Kurse und Workshops mit Unternehmen, Verbänden und Verwaltungen. Es stellt kostenlos Wissen in Form von White Papers, Checklisten, Anleitungen usw. zur Verfügung. Im Bereich der angewandten Forschung arbeitet das Institut an Projekten für Auftraggeber aus der Wirtschaft, der öffentlichen Verwaltung oder für NGOs. Dabei kommt eine der grossen Stärken der HWZ zum Tragen: die lösungsorientierte Arbeitsweise, die auch im Unterricht hervorgehoben wird.

www.fh-hwz.ch/idb

Ihr Kontakt

Studiengangsleiter

Ralph Hutter
Head Product Management Ecosystems, Finnova AG

Am Institute for Digital Business HWZ ist Ralph verantwortlich für die Produkt Entwicklung der MAS / CAS Angebote sowie die Forschungsaktivitäten. Daneben führt es als Studiengangsleiter den CAS Cyber Risk & Security HWZ und den CAS Mobile Business and Ecosystems HWZ.

Der diplomierte Informatiker mit MBA-Abschluss hat über 20 Jahre Berufserfahrung in Digitalisierungsprojekten bei Schweizer Banken und führenden Software-Herstellern. Hauptberuflich arbeitet er als Head Product Management Ecosystems bei Finnova. Seit 2009 doziert er an der HWZ in CAS-, MAS- und EMBA-Studiengängen und ist Studiengangsleiter von verschiedenen CAS-Studiengängen.

Seine Freizeit verbringt er vorzugsweise mit Geocaching, analogen Fotoapparaten und auf dem Fahrrad. Er backt leidenschaftlich gerne Brot.

Ralph Hutter
ralph.hutter@fh-hwz.ch

Auskunft/Beratung

Für allgemeine Informationen zur HWZ und zu diesem Studium wenden Sie sich bitte an das Master-Sekretariat:
043 322 26 88, master@fh-hwz.ch.

Vertiefende Fragen beantwortet Ihnen der Studiengangsleiter gerne. Er steht Ihnen auch für ein persönliches Beratungsgespräch zur Verfügung. Bitte vereinbaren Sie online oder telefonisch einen Termin über das Master-Sekretariat.

Informationsveranstaltungen
Aktuelle Daten finden Sie auf
www.fh-hwz.ch/infoabende.

Check-in

Für Ihre Anmeldung benutzen Sie bitte das entsprechende Formular auf unserer Website:

www.fh-hwz.ch/cascrs

«Die Nachlässigkeit im Umgang mit eigenen Daten und der IT-Sicherheit wird in einem CAS DRM vor Augen geführt. Mit den Tipps der Dozierenden kann ich heute meine Privatsphäre viel besser schützen und bewege mich viel umsichtiger im WWW.»

Max Keller
Risk Management Consultant,
Funk Insurance Brokers AG