Cyber Security instructor-led training in Switzerland, Liechtenstein, and Germany 2020
Table of contents

A. About us, page 4.
B. Events and open instructor-led training, page 6.
C. On-site instructor-led training programs in Switzerland, Liechtenstein, and Germany, page 7.
C3. The target is the bank: From hacking to cybercrime to cyberespionage, page 12.
C4. State-sponsored but independent hacking groups. The new long arm of a country that exploits legal pluralism and makes the law a strategic instrument, page 16.
C5. Deception, disinformation, misinformation, propaganda, and direct democracy, page 19.
C8. Cybersecurity awareness and training, for managers and employees working in Swiss hotels and Swiss subsidiaries of hotel chains, page 33.
C9. Tailored cybersecurity awareness and training for managers and employees working in the commercial and private aviation, page 37.
C11. The General Data Protection Regulation (GDPR) for the Board of Directors and the CEO of Swiss and non-EU based companies, page 44.


C16. Your program, page 69.


E. Contact us, page 73.
A. About us

Cyber Risk GmbH has been established in Horgen, Switzerland by George Lekatis, a well-known expert in risk management and compliance. George is the general manager of Compliance LLC, incorporated in Wilmington NC and offices in Washington DC, a provider of risk and compliance training and executive coaching in 36 countries.

Several business units of Compliance LLC are very successful associations that offer standard, premium and lifetime membership, weekly or monthly updates, training, certification, Authorized Certified Trainer (ACT) programs and other services to their members. George is the president of the International Association of Risk and Compliance Professionals (IARCP, www.risk-compliance-association.com). He oversaw the team that developed the Certified Risk and Compliance Management Professional (CRCMP) program. Companies and organizations like Accenture, USAA etc. consider the CRCMP a preferred certificate.

George has more than 20,000 hours experience as a seminar leader. He has provided training and executive coaching in information security and risk management to many leading global organizations, especially banks and insurance firms, in 36 countries. You can find some testimonials at: www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf
George holds a Master of Laws in international business law from the University of London (Queen Mary, UCL). He started his career as a mathematician. He also holds 60 professional certificates in IT, information security and risk management. He has become a Certified Information Systems Security Professional (CISSP), CISSP lead instructor, Steganography Investigator, Internet Security Systems (ISS) Certified in Internet Scanner, Database Scanner and System Scanner, Checkpoint Certified Security Administrator (CCSA), Microsoft Certified System Engineer (MCSE), Microsoft Certified Trainer (MCT). As an expert witness and litigation consultant, he is qualified to investigate and testify about risk and compliance management standards and due diligence.
B. Events and open instructor-led training programs

The world of cyber security and privacy is constantly changing. Our events and open classes have the objective to help organizations, firms and persons stay on top of those changes. We publish our events and open classes at the Facebook and LinkedIn pages of Cyber Risk GmbH. You may visit:

www.facebook.com/CyberRiskSwitzerland
www.linkedin.com/groups/8531503/
C. On-site instructor-led training programs in Switzerland, Liechtenstein, and Germany.

C1. Cyber Risk Awareness and Training for the Swiss branches and subsidiaries of international firms.

Overview

Swiss branches and subsidiaries of international firms must comply with cyber security and privacy laws, regulations, international standards, and best practices that respect the specific requirements of the countries where they sell products and provide services.

Managers and employees must understand the enterprise wide risk management requirements, and must meet the expectations of Switzerland, Europe, the United States, and other countries.

Target Audience

The program is beneficial to managers and employees working in Swiss branches and subsidiaries of international firms.

Duration

Half day (09:00-13:00) to one day (09:00-17:00), depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.
Instructor

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf

Language

English

We will discuss:

- The Federal Council’s national strategy for the protection of Switzerland against cyber risks (NCS) of June 2012, its implementation plan (IP NCS) of May 2013, the Swiss specific requirements, and the developments in Switzerland.

- The follow-up strategy (2018-2023).

- The critical infrastructure protection principles in Switzerland, the USA, the EU, and other countries.

- The US Executive Orders, and the EU Cybersecurity Strategy and Directives that are important for cyber risk management.

- The cyber risk management strategy and policies that satisfy the requirements in Switzerland, the USA, the EU, and other countries.
C2. Cyber Risk Awareness and Training for the Board of Directors and the CEO of Swiss branches and subsidiaries of international firms.

Overview

Threat networks are flexible, agile, and ever-evolving groupings of hackers, criminals, terrorists, competing countries and their supporters and facilitators. These networks could include employees, competitors, suppliers, and service providers that blend illicit activity with licit business.

The Board and the CEO must have the knowledge and skills necessary to exercise professional judgment in assessing cybersecurity risks, challenging security plans, discussing activities, formulating opinions, and evaluating policies and solutions that protect the assets of their organization.

The failure to maintain adequate risk oversight can expose companies, officers, and directors to liability. Directors owe fiduciary duties to their shareholders and have a significant role in overseeing the risk management of the company. The failure to exercise appropriate oversight in the face of known risks constitutes a breach of the duty of loyalty. A decision about cybersecurity that was “ill-advised or negligent” constitutes a breach of the duty of care.

The Board and the CEO must also assess whether and how to disclose a cyberattack internally and externally to customers and investors. After a successful cyberattack, companies and organizations must provide evidence that they have an adequate and tested cybersecurity program in place that meets international standards, and that they are prepared to respond to a security breach properly and quickly.

Target Audience

The program is beneficial to the Board of Directors and the CEO of Swiss branches and subsidiaries of international firms.

Duration

2 hours to half day, depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

Instructor


Language

English

We can discuss:

* **Understanding the threat**
  - Cybersecurity is not simply a technical or a technology issue.
- Perpetrators: From disgruntled employees to competitors to organized crime to nation states.

*Overview of the art and the science to prevent and detect hacking, cybercrime, and cyberespionage*
- Foreign collection efforts and espionage that targets technology, intellectual property, trade secrets and proprietary information. What can we do?
- When the most dangerous adversary becomes the primary hardware manufacturer.
- Criminal organizations and secondary markets for sensitive information.
- Cyber terrorism: A computer-based attack or threat of attack, intended to intimidate, or coerce governments or organizations in pursuit of goals that are political, religious, or ideological.

*Defending our organization and the Swiss critical infrastructure in cyberspace*
- The Federal Council’s national strategy for the protection of Switzerland against cyber risks (NCS) and its implementation plan (IP NCS).
- Understanding the government's expectations.
- Protecting clients’ sensitive data, infrastructure and competitive advantage.
- Exchanging information and cooperating with the public sector.
- Critical infrastructure protection principles.
- International standards and best practices in Switzerland, the USA, and the European Union.

*Cybersecurity Risk Management for the Board of Directors and the CEO*
- What company assets must be protected and why.
- Understanding cyber risks, the company’s plan to manage these risks, and the company’s response plan when a breach occurs.
- Assessing the reputational risk and the legal exposure after a cyber incident.
- Is there a Board committee assigned to address cybersecurity?
- Does someone serving on the Board have expertise in cybersecurity and information technology?
- The Board must be informed on the company’s cyber risks and proactively oversee the company’s management of cyber risks.
- The Board must evaluate whether the company is properly managing cyber risks, including whether adequate resources are devoted to cybersecurity.
- The Board must understand the risk at the level of outsourced providers and contractors. Which are the policies in place?
- Cybersecurity budget.
- Exchanging information. What are circumstances when law enforcement will be notified?
- When cybersecurity breaches are disclosed to investors?
- Creating a culture of awareness: Security awareness training covering cybersecurity risks and policies.

Meeting international standards - The list of cyber security questions for CEOs created by the Department of Homeland Security in the USA:

- How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
- What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
- How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
- How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
- How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Closing

- Examples and case studies.
- Closing remarks.
C3. The target is the bank: From hacking to cybercrime to cyberespionage

The exploitation of IT vulnerabilities or the use of deceptive or manipulative attacks on people to gain access to facilities, systems, and the critical infrastructure.

Overview

Critical Infrastructure consists of systems and assets, whether physical or virtual, so vital to a country, that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The globally-interconnected digital information and communications infrastructure known as “cyberspace” underpins almost every facet of modern society and provides critical support for the economy. Yet, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century.

The digital infrastructure’s architecture was driven more by considerations of interoperability and efficiency than of security. The cyber threat to the financial sector as an important part of the critical infrastructure continues to grow and represents one of the most serious financial and national security challenges banks and countries confront.

The number of cyber-attacks directed at financial institutions of all sizes is growing. Cyber risks, like reputational and financial risks, affect a bank’s bottom line. Beyond the impact to an individual
bank, cyber risks have far-reaching economic and national security consequences. It is important to ensure that banks maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality and privacy.

**Target Audience**
The program includes problem-solving exercises and role-plays. It is beneficial to:

- Managers and employees working at the strategic, tactical, and operational levels of risk, compliance, IT, and information security of a bank.
- Risk, compliance, IT, and information security managers, employees, auditors, and consultants.
- Network, systems, and security administrators.
- Vendors, suppliers, and service providers.
- Incident handlers and incident response professionals.
- Threat analysts.
- Vulnerability assessment personnel.

**Duration**
One day (09:00-17:00). We can tailor the program to meet specific requirements.

**Instructor**
Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Language**
English

**Course Synopsis**

*Step 1 – Collecting information about persons and systems*

- Reconnaissance: The research phase used to identify and select targets.
- Looking for information about the systems of a bank.
- Looking for information about the persons working in a bank or for a bank.
- Outsourcing and budget cuts can have hidden costs.
- Gathering information through recruitment of former employees, suppliers, consultants, or service providers.
- Who has signed a confidentiality agreement? A good list of prime targets for all adversaries.
- Contract information (bid, proposal, award).
- Looking at our daily activities from the adversaries' point of view.
- More prime targets: Disgruntled employees, ideologists, employees having a lavish lifestyle, employees having “weaknesses”, lawyers having access to trade secrets and sensitive information.
- Countermeasures: What banks must do.

**Step 2 – Identifying possible targets and victims**
- Hardware attacks, software attacks.
- We always purchase branded and genuine hardware components (to the best of our knowledge), but our adversaries can exploit this pattern.
- Malicious hardware modifications: Acquiring hardware components with a backdoor, and how it affects all other information security policies.
- Phishing, social phishing, spear phishing, watering hole attacks.
- Which systems and which persons? The hit list.

**Step 3 – Evaluation, recruitment, and testing**
- Exploiting vulnerabilities in systems.
- Collecting more information about persons.
- The problem with the sleeping agents.
- Blackmailing employees: The art and the science.
- Testing the asset.
- Case studies and lessons learned.
- Countermeasures: What banks must do.

**Step 4 - Privilege escalation**
1. Systems:
   - A. Vertical privilege escalation, where adversaries grant themselves higher privileges.
   - B. Horizontal privilege escalation, where adversaries use the identity of other users with similar privileges.
   - Obtaining customer account details.
   - Internal information, social engineering.
   - Creating backdoors.
   - Covering their tracks.
2. Persons:
   - Exploiting the human networks.

**Step 5 – Identifying important clients of the bank**
- Important clients working in the public and the private sector.
- Repeating the process - Steps 1 to 4.

**Step 6 – Critical infrastructure**
- Creating backdoors.
- Covering their tracks.
- Ticking time bombs and backdoor triggers based on specific input data.

**Overview of the art and the science to prevent and detect hacking, cybercrime, and cyberespionage**
- Foreign collection efforts and espionage that targets technology, intellectual property, trade secrets and proprietary information. What can we do?
- When the most dangerous adversary becomes the primary hardware manufacturer.
- Criminal organizations and secondary markets for sensitive information.
- Cyber terrorism: A computer-based attack or threat of attack, intended to intimidate, or coerce governments or organizations in pursuit of goals that are political, religious, or ideological.

**Defending our bank and the Swiss critical infrastructure in cyberspace**
- The Federal Council's national strategy for the protection of Switzerland against cyber risks (NCS) and its implementation plan (IP NCS).
- Understanding the government's expectations.
- Protecting clients’ sensitive data, infrastructure and competitive advantage.
- Exchanging information and cooperating with the public sector.
- Critical infrastructure protection principles.
- International standards and best practices in Switzerland, the USA, and the EU.
- Closing remarks.
C4. State-sponsored but independent hacking groups. The new long arm of a country that exploits legal pluralism and makes the law a strategic instrument.

Overview

According to Article 51 of the U.N. Charter: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”

But, is a cyber-attack comparable to an armed attack?

There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Nations assert different definitions and apply different thresholds for what constitutes a use of force.

For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under jus ad bellum, then such cyber operations would likely also be regarded as a use of force.

Important weaknesses of international law include the assumption that it is possible to isolate military and civilian targets with sufficient clarity, and to distinguish a tangible military objective
to be attained from an attack.

More than 20 countries have announced their intent to use offensive cyber capabilities, in line with Article 2(4) and Article 51 of the United Nations (UN) Charter.

Unfortunately, these capabilities will not help when the attackers are State-sponsored groups, and the States supporting them, claim that not only they are not involved, but also that their adversaries (the victims) have fabricated evidence about it. This is a very effective disinformation operation.

Adversaries have already successfully exploited weakness of non-authoritarian societies, especially the political and legal interpretation of facts from different political parties. It’s difficult to use offensive cyber capabilities in line with democratic principles and international law, as it is almost impossible to distinguish with absolute certainty between nation-state attacks and attacks from state-sponsored independent groups.

Even when intelligence services know that an attack comes from a State that uses a state-sponsored independent group, they cannot disclose the information and the evidence that supports their assessment, as disclosures about technical and physical intelligence capabilities and initiatives can undermine current and future operations. This is the “second attribution problem” – they know but they cannot disclose what they know.

As an example, we will discuss the data breach at the U.S. Office of Personnel Management (OPM). OPM systems had information related to the background investigations of current, former, and prospective federal government employees, U.S. military personnel, and those for whom a federal background investigation was conducted. The attackers now have access to information about federal employees, federal retirees and former federal employees. They have access to military records, veterans' status information, addresses, dates of birth, job and pay history, health insurance and life insurance information, pension information, data on age, gender, race, even fingerprints.

But why?

Aldrich Ames, a former intelligence officer turned mole, has said: “Espionage, for the most part, involves finding a person who knows something or has something that you can induce them secretly to give to you. That almost always involves a betrayal of trust.”

Finding this person is much easier, if you have data easily converted to intelligence, like the data stolen from the U.S. Office of Personnel Management (OPM). This leak is a direct risk for the critical infrastructure.

There are questions to be answered, and decisions to be made, not only about tactic and strategy, but also political and legal interpretation.

We tailor the program to meet specific requirements. You may contact us to discuss your needs.

Target Audience

The program is beneficial to the Board of Directors, the CEO, and senior management of firms and
organizations of the private and the public sector.

Duration
1 hour to half day, depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

Instructor

Language
English
C5. Deception, disinformation, misinformation, propaganda, and direct democracy.

“For where the lion’s skin will not reach, you must patch it out with the fox’s.”

Lysander the Spartan

Overview

*Misinformation* is incorrect or misleading information.

*Disinformation* is false information, deliberately and often covertly spread, in order to influence public opinion, or obscure the truth.

*Propaganda* is a broader and older term. Propaganda uses disinformation as a method. While the French philosopher Jacques Driencourt asserted that everything is propaganda, the term is most often associated with political persuasion and psychological warfare.

*Psychological warfare* is the use of propaganda against an enemy (or even a friend that could become an enemy in the future), with the intent to break his will to fight or resist, or to render him favorably disposed to one's position.

In *deception* (according to Bell and Whaley), someone is showing the false and hiding the real. Hiding the real is divided into masking, repackaging, and dazzling, while showing the fake is divided into mimicking, inventing, and decoying.

*People are remarkably bad at detecting deception and disinformation.*
They often trust what others say, and usually they are right to do so. This is called the “truth bias”. People also tend to believe something when it is repeated. They tend to believe something they learn for the first time, and subsequent rebuttals may reinforce the original information, rather than dissipate it.

Humans have an unconscious preference for things they associate with themselves, and they are more likely to believe messages from users they perceive as similar to themselves. They believe that sources are credible, if other people consider them credible. They trust fake user profiles with images and background information they like.

Citizens must understand that millions of fake accounts follow thousands of real and fake users, creating the perception of a large following. This large following enhances perceived credibility, and attracts more human followers, creating a positive feedback cycle.

People are more likely to believe others who are in positions of power. Fake accounts have false credentials, like false affiliation with government agencies, corporations, activists, and political parties, to boost credibility.

Freedom of information and expression are of paramount importance in many cultures. The more freedom of information we have, the better. But the more information we have, the more difficult becomes to understand what is right and what is wrong. The right of expression and the freedom of information can be used against the citizens. We often have the weaponization of information.

The Internet and the social media are key game-changers in exploiting rights and freedoms. In the past, a secret service should work hard to get disinformation in the press. Today, the Internet and the social media give the opportunity for spreading limitless fake photos, reports, and "opinions". Many secret services wage online wars using Twitter, Facebook, LinkedIn, Google+, Instagram, Pinterest, Viber etc. Only imagination is the limit.

Social media platforms, autonomous agents, and big data are directed towards the manipulation of public opinion. Social media bots (computer programs mimicking human behaviour and conversations, using artificial intelligence) allow for massive amplification of political views, manufacture trends, game hashtags, add content, spam opposition, attack journalists and persons that tell the truth.

In the hands of State-sponsored groups these automated tools can be used to both boost and silence communication and organization among citizens.

Over 10 percent of content across social media websites, and 62 percent of all web traffic, is generated by bots, not humans. Over 45 million Twitter accounts are bots, according to researchers at the University of Southern California.

*Machine-driven communications tools (MADCOMs)* use cognitive psychology and artificial intelligence based persuasive techniques. These tools spread information, messages, and ideas online, for influence, propaganda, counter-messaging, disinformation, espionage, intimidation. They use human-like speech to dominate the information-space and capture the attention of citizens.
Artificial intelligence (AI) technologies enable computers to simulate cognitive processes, such as elements of human thinking. Machines can make decisions, perceive data or the environment, and act to satisfy objectives.

The rule of the people, by the people, and for the people, requires citizens that can make decisions in areas they do not always understand. When citizens understand the online environment, they will be way more prepared to protect their families, their working environment, and their country.

**Target Audience**

The program is beneficial to the Board of Directors, the CEO, and senior management of firms and organizations of the private and the public sector.

**Duration**

1 hour to half day, depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

**Instructor**


**Language**

English
Social engineering

“While we focus the vast majority of our security efforts on protecting computers and networks, more than 80% of cyber attacks and over 70% of those from nation states are initiated by exploiting humans rather than computer or network security flaws.”

*The Active Social Engineering Defense (ASED) program,* DARPA

Cybersecurity is not only a technical challenge. It is also a behavioral challenge. As long as managers and employees can provide access to systems and data, cybersecurity depends on them too.

Employees that have access to critical assets of an organization, become targets. Those that have access to technology and organizational assets are also responsible for the protection of those assets. Are they fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations?

A major challenge in today’s cyber security efforts is the lack of awareness and training. Many organizations and companies of the public and the private sector continue to believe that cyber security is a technical, not a strategic discipline. They believe that cyber security involves only the protection of systems from threats like unauthorized access, not the awareness and training of persons that have authorized access to systems and information.

That becomes an exploitable organizational vulnerability. Hackers prefer attacking humans, because it is simpler. While technology keeps advancing and security systems become stronger and more complicated to compromise, human psychology has remained the same over centuries and is thus easier to exploit.

The stimulus-response effect in human vulnerabilities is consistent, and exploiting these
vulnerabilities is consistently successful. In addition, it is often a low-cost, low-risk, and high-reward approach.

While computer hacking does involve the manipulation of technology as a means of enabling illegal activity, social engineering involves the manipulation of humans and other non-technical elements as a means of breaching organizational security.

Social engineering is the art and science of skillfully manipulating other people into taking specific actions that assist an attacker in successfully initiating and completing an attack.

Social engineering tactics can be as simple as convincing someone to click on a URL, or as advanced as convincing someone to provide information, or to take action that will enable a breach.

The most exploited factor in social engineering, is ignorance. A person that does not know the tactics and methods used from social engineers, is defenseless against them. Understanding how social engineers achieve their objectives is the strongest counter-measure against social engineering attacks.
C6. Social Engineering: Awareness and Defense

Overview

In this course, managers and employees learn to understand, identify and respond to social engineering attacks. The program provides with the knowledge necessary to recognize the most typical and frequently used types of attacks, and explains how to respond. During the course, attendees learn why security should supersede convenience at all times, and why policy needs to be diligently followed. Defense mechanisms and countermeasures are included in each section. We can tailor the course to meet specific requirements. No previous knowledge is required.

Target Audience

The program is beneficial to managers and employees working in companies and organizations of the public and the private sector.

Duration

Half day to 2 days. We tailor the program to meet specific requirements.

Instructor

Christina Lekati, psychologist, social engineering expert. To learn about her you may visit:
www.social-engineering-training.ch/About_Christina_Lekati.html


**Language**

English

**Course Synopsis:**

*Introduction.*

1. Security is not a technical issue alone.
2. The importance of cultivating and maintaining security habits.
3. Non-technical means that protect your infrastructure.
4. Having multiple layers of security.

*Social Engineering.*

1. What is social engineering.
2. Why social engineering is a primary attack vector — and why it is likely you will encounter it, too.
3. How does social engineering work?
4. What do attackers prey upon?
5. The numbers game vs. highly tailored and targeted attacks.

*Who is the attacker?*

1. Possible adversaries: competitors, employees, individuals, small groups, insiders, service providers, criminal organizations, nation states.
2. Social engineering is a business, and a full-time profession.

*The Social Engineering Kill-chain.*

1. Reconnaissance: The research phase used to identify and select targets.
2. Targeting: Who is the most vulnerable person to attack? What is the biggest vulnerability of the target?
3. Pretexting: The attacker’s cover story.
4. Establishing trust with the target.
5. Manipulating, exploiting and victimizing.
6. Case studies.

*Typical Social Engineering Attacks from a Distance.*

1. Phishing Emails.
2. Spear Phishing.
3. Vishing.
4. Smishing.
5. Watering Holes.
7. Baiting.
8. Whaling phishing.
9. Emotional triggers that will make you want to respond - but you shouldn’t.
10. Case studies.

Is your social media content making you a target?
1. Social media is a primary source of information for attackers.
2. How your social media content can be used against you.
3. Cybersecurity hygiene advice for social media.
4. Attacks through social media.
5. Examples.

In-Person attacks and manipulation techniques.
1. USB traps.
2. Emotional elicitation & exploitation.
3. Time pressure.
4. Authority.
5. Likeability.
6. Intimidation.
7. Reciprocity.
8. Impersonation.
10. Commitment & Consistency.

Physical security.
1. Why social engineers will try to enter your establishment.
2. What assets can be stolen/ compromised?
3. Gaining unauthorized access to physical spaces.
4. Tailgating and bypassing physical security measures.
5. Locked does NOT mean secure - lockpicking capabilities.

Identifying a social engineering attack.
1. Identifying manipulation and deceit.
2. Emotional triggers, emotional exploitation & what to do about it.
3. Verifying intentions - subtly.
4. Case studies.

5. Responding to and deterring a social engineering attack.

_Policies & Procedures._

1. Convenience vs security.

2. What policies? What procedures? Why?

3. Using & applying policy to your advantage: escaping manipulation and uncomfortable situations.


5. Disgruntled employees.

6. Best practices for third party vendors entering the establishment.

_Developing information security habits._

1. Developing and internalizing everyday security habits.

2. Maintaining helpfulness without compromising security.

3. Establishing healthy boundaries in communication.

_Concluding Remarks._

Our ultimate goal is to develop and strengthen an essential layer of organizational security, the human one (or as commonly called “the human firewall”), that will support and protect the assets of a company or organization.
C7. Practical Social Engineering Defense: Protection of Sensitive Information

Overview

This course is important for governmental or non-governmental organizations and companies handling sensitive or classified information - a powerful, high-value asset that attracts many attackers.

Are the managers and employees handling this information ready to protect it and to respond to potential threats and attacks?

This program offers attendees the skills and knowledge necessary to identify potential threats and respond to them.

Target Audience

The program is beneficial to managers and employees working in companies and organizations of the public and the private sector.

No previous knowledge is required. We can tailor the course to meet specific requirements. This program can include exercises and role playing.

Language

English

Instructor

Christina Lekati, psychologist. To learn about her you may visit: www.social-engineering-training.ch/About_Christina_Lekati.html

Duration

Half day to 2 days. We tailor the program to meet specific requirements.
Course Synopsis:

What Is Considered Sensitive Information?
1. What the organization vs. what the attacker considers to be valuable information.
2. Personal information.
3. Classified Information.
4. Information about the organization.

Who is the Attacker and why?
1. Possible adversaries: criminal organizations, nation states, activists, individuals, small groups, insiders.
2. Social engineering is a business, a full-time profession.
3. Selling information in the dark web.
4. Using information to sabotage operations, for reputational damage, for destruction, and more.

Social Engineering Methods for Information Harvesting.
1. Building a personal relationship with the target.
2. Human Intelligence (HUMINT).
3. Open Source Intelligence (OSINT).
4. Geospatial Intelligence (GEOINT).
5. Communications Intelligence (COMINT).
6. Special Issue: the surprising quality of intelligence gathered from inference espionage.
7. Threading them together.

Long term vs short term attack efforts.
1. Short term efforts.
2. Long term efforts: overt and covert asset cultivation.

Social Engineering (SE) Modus Operandi.
Step 1: Reconnaissance.
1. Information Harvesting.
2. In-depth OSINT: Everything that can be found about you.
3. Turning information into intelligence: how even seemingly innocent and irrelevant pieces of information are puzzled together.
4. Profiling targets.
5. Selecting targets.
6. Identifying objectives.

SE Modus Operandi Step 2: Pretexting.
1. Crafting a strategy based on the target’s profile.
2. Constructing the attacker’s persona.
3. Mirroring or complementing the target’s personality.
4. Cover story.
5. Tailoring the attack.

SE Modus Operandi Step 3: Building a Relationship.
1. Identifying potential occasions for initiating contact.
2. Getting into the circle of awareness.
3. Initiating contact and hooking the target.
4. Building trust and credibility.
5. Their personality will match yours... almost perfectly.
6. “What are the chances! To meet someone like you...”.
7. Frequent high-value contact.
8. Privilege escalation.
9. Study cases.

SE Modus Operandi Step 4: Exploitation.
1. Stretching the boundaries: escalating from obtaining slightly significant pieces of information to increasingly more important ones.
2. Links, attachments and USBs with malicious code.
3. Obtaining information for other high-value targets.
4. Launching specific attacks (variety of possibilities).
5. Study Cases.

**Frequently Used Influence Tactics.**
1. Situational reframing.
2. Satisfying the target’s personal motives and interests.
3. Satisfying the target’s unmet needs.
4. Seduction techniques.
5. Mystery.
6. Familiarity and likeability.
7. The “Feel good” influence factor.
8. The “Halo Effect”.

**Frequently used Information Extortion Techniques.**
1. Elicitation.
2. Putting the target in a trance.
3. The magnet effect: how using one piece of information can elicit more.
4. Covertly cultivating a sense of obligation to answering questions.
5. Exploiting compliance.

**The Social Engineer’s Target Management.**
1. Targets (assets) that respond and deliver a high ROI – are to be maintained.
2. Targets that hold highly valuable information – are to be cultivated.
3. Targets that do not respond, do not deliver or are suspicious – are to be abandoned.
4. You want to be in the third category.

**Frequently Used Scenarios.**
1. The “Damsel in Distress”.
2. Romance Fraudsters.
3. The Rescuer.
4. Direct approach with value proposition.

**Defense: Know Thyself.**
1. The tendency to verify your wished-for scenario and self-induced blindness.
2. The tendency to justify your guilty actions.
3. Know your weaknesses.
4. Believing it will not happen to you.
5. We are inherently bad at detecting deceit.

Defense: Further Countermeasures.
1. Lessons from the field of counterintelligence.
2. The biggest weakness of a social engineer.
3. Using their toolkit against them.
4. Verifying claims.
5. Maintaining boundaries in communication.
6. Handling emotional triggers.
8. New hiring standards.

Attacker Detection Checklist.
Concluding Remarks.
C8. Cybersecurity awareness and training, for managers and employees working in Swiss hotels and Swiss subsidiaries of hotel chains.

Overview

For decades, when we were using the words “hotel security”, we were usually referring to “physical security”. It was all about guest protection, locks, safes, and surveillance.

Guests and hotel employees today expect that the same level of protection extends to the digital assets that reside not only on their laptops and smartphones, but also on the hotel’s systems. Hotels are obliged to respect this expectation, especially after the new privacy regulations, including the General Data Protection Regulation (GDPR) and the revised Data Protection Act (DPA), which must be equivalent to the GDPR.

Swiss hotels and Swiss subsidiaries of hotel chains must comply with cyber security and privacy laws and regulations, and must follow international standards and best practices that protect their guests and employees.
A new cybersecurity culture is necessary. It refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, values and expectations of hotel guests regarding cybersecurity. Cybersecurity awareness for all managers and employees of a hotel is necessary, in order to make information security considerations an integral part of an employee’s job, habits and conduct, embedding them in their day-to-day actions.

We tailor the program to meet specific requirements. You may contact us to discuss your needs.

**Target Audience**

The program is beneficial to all managers and employees working in Swiss hotels, and Swiss subsidiaries of hotel chains.

**Duration**

Half day (09:00-13:00) to one day (09:00-17:00), depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

**Instructor**

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Language**

English

**This program covers:**

- Important developments in the hospitality industry after the new privacy regulations, including the GDPR and the revised Data Protection Act (DPA).
- Understanding the challenges.
- Hotels, and the report from the Federal Intelligence Service (FIS), “Switzerland’s Security 2018”.
- Hotels, and the report from the Federal Council, "National Strategy for the Protection of Switzerland Against Cyber Risks".
- *Who is the “attacker”?*
- Countries, organizations, criminal organizations, small groups, individuals, employees, insiders, service providers.
- Hacktivists and the hotel industry.
- Professional criminals and information warriors.
- *How they attack hotels?*
- Step 1 – Collecting information about persons and systems.
- Step 2 – Identifying possible targets and victims.
- Step 3 – Evaluation, recruitment and testing.
- Step 4 - Privilege escalation.
- Step 5 – Identifying important clients and VIPs.
- Step 6 – Critical infrastructure.
- Employees and their weaknesses and vulnerabilities.
- Employee collusion with external parties.
- Blackmailing employees: The art and the science.
- Romance fraudsters and webcam blackmail: Which is the risk for the hotel?
- Specific risks for the hospitality industry, and best practices to protect the hotel.
- What guests need, and which are the cyber risks?
  - a. Speed and convenience.
  - It is difficult to balance speed, convenience and security.
  - b. Effective and efficient web site and reservation system.
  - Examples of challenges and risks.
  - c. Great customer service.
  - Example - how it can be exploited.
  - d. A nice room and housekeeping.
  - Example - “The cleaning staff’s hack”.
  - e. Food, drinks and entertainment.
  - Point-of-sale (POS) fraud and challenges.
  - Credit card cloning.
  - f. Internet access.
  - Honeypots, rogue access points, man-in-the-middle attack.
  - g. Security.
  - Unauthorized access is a major problem, and social engineering is a great tool for attackers.
  - h. Privacy.
  - The hotel industry is considered one of the most vulnerable to data threats.
  - i. Money (if they can sue the hotel for negligence...).
- What must be protected?
- Best practices for managers and employees in the hospitality industry.
- What to do, what to avoid.
- From customer satisfaction vs. cyber security, to customer satisfaction as the result of cyber security.
- The DarkHotel group.
- **Malware.**
- Trojan Horses and free programs, games and utilities
- Ransomware.
- **Social Engineering.**
- Reverse Social Engineering.
- Common social engineering techniques.
- 1. Pretexting.
- 2. Baiting.
- 4. Tailgating.
- **Phishing attacks.**
- Spear-phishing.
- Clone phishing.
- Whaling – phishing for executives.
- Smishing and Vishing Attacks.
- **Cyber Hygiene.**
- The online analogue of personal hygiene.
- Personal devices in the hotel.
- Untrusted storage devices.
- **Case studies.**
- InterContinental, Wyndham, Starwood, Hyatt, Hilton, Romantik Seehotel Jägerwirt.
- What has happened?
- Why did it happen?
- Which were the consequences?
- How could it be avoided?

Closing remarks and questions.
C9. Tailored cybersecurity awareness and training for managers and employees working in the commercial and private aviation.

Overview

For decades, when we were using the words “airline security” or “aviation security”, we were usually referring to unlawful seizure of aircrafts, destruction of aircrafts, hostage-taking, forcible intrusion, weapons or hazardous devices intended for criminal purposes, or use of an aircraft for criminal purposes or terrorism.

Cybersecurity is the new challenge for the aviation industry.

Customers and employees of commercial or private aviation today expect that the same level of protection extends to the digital assets that reside on aviation systems. Airlines are obliged to respect this expectation, especially after the new privacy regulations, including the General Data Protection Regulation (GDPR).

The commercial and private aviation must comply with cyber security and privacy laws and regulations, and must follow international standards and best practices that protect their customers and employees.

A new cybersecurity culture is necessary. It refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, values and expectations of customers regarding cybersecurity.

Aircraft cybersecurity involves the policies, procedures, awareness and training for the prevention, detection, and response to deliberate malicious acts that target systems, persons (via social
Airport cybersecurity involves the policies, procedures, awareness and training for the prevention, detection, and response to deliberate malicious acts that target systems, persons (via social engineering) and data, to compromise an airport's systems and staff.

During the past decades, airlines have made substantial investments in information technology solutions that contribute to improved operational efficiency, safety, and customer satisfaction. The more complex and interconnected the systems, the more awareness and training is required for all managers and employees that use these systems.

Cybersecurity awareness for all managers and employees in the commercial and private aviation is necessary, in order to make information security considerations an integral part of every job, habits and conduct, embedding them in their day-to-day actions.

We tailor the program to meet specific requirements. You may contact us to discuss your needs.

**Target Audience**

The program is beneficial to managers and employees working in the commercial and private aviation.

**Instructor**

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Duration**

Half day (09:00-13:00) to one day (09:00-17:00), depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

**Language**

English

**Modules of the tailor-made training**

- Important developments in the commercial and private aviation industry after the new privacy regulations, including the GDPR.
- Understanding the challenges.
- Cyber threats to the aviation industry.
- Cyber-attacks against passengers, baggage, cargo, catering, systems, staff.
- Who is the attacker?
- Possible adversaries: Countries, competitors, criminal organizations, small groups, individuals, employees, insiders, service providers.
- Hacktivists and the commercial and private aviation industry.
- Professional criminals and information warriors.
- Step 1 – Collecting information about persons and systems.
- Step 2 – Identifying possible targets and victims.
- Step 3 – Evaluation, recruitment and testing.
- Step 4 - Privilege escalation.
- Step 5 – Identifying important clients and VIPs.
- Step 6 – Critical infrastructure.

- Employee collusion with external parties.
- Blackmailing employees: The art and the science.
- Romance fraudsters and webcam blackmail: Which is the risk for the aviation industry?
- Trojan Horses and free programs, games and utilities.
- Ransomware.
- Social Engineering.

- Reverse Social Engineering. Common social engineering techniques
  - 1. Pretexting.
  - 2. Baiting.
  - 4. Tailgating.

- Phishing attacks.
- Spear-phishing.
- Clone phishing.
- Whaling – phishing for executives.
- Smishing and Vishing Attacks.

- Point-of-sale (POS) fraud and challenges.
- Credit card cloning.
- Honeypots, rogue access points, man-in-the-middle attack.

- What customers need, and which are the cyber risks?
- Examples of challenges and risks.
- From customer satisfaction vs. cybersecurity, to customer satisfaction as the result of cybersecurity.

- Cyber Hygiene.
- The online analogue of personal hygiene.
- Personal devices.
- Untrusted storage devices.

- Case studies. Cyber-attacks against airport operators, aviation authorities, airlines, and air navigation service providers.

You may contact us to discuss your needs.
C10. The General Data Protection Regulation (GDPR) for Swiss and non-EU based companies: The new privacy and security requirements

Overview
The GDPR is applicable for Swiss and non-EU companies that are offering goods or services to identified or identifiable EU natural persons ("data subjects"), organizations processing personal data of EU data subjects, or organizations that monitor the online behaviour of EU data subjects. Non-EU companies that have no local presence in the EU are also in the scope of the GDPR legislation.

Target Audience:
The program is beneficial to:
- Managers and employees working at the strategic, tactical, and operational levels of risk management, compliance, information security and IT management.
- Data protection and privacy managers, employees, auditors, and consultants.
- Marketing managers and persons involved in profiling.
Controllers and processors.

- Vendors, suppliers, and service providers.

**Duration:**
Half day (09:00-13:00) to one day (09:00-17:00), depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

**Instructor**
Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Language:**
English

**Course Synopsis:**

*Understanding the General Data Protection Regulation (GDPR)*

- An overview of the GDPR.
- What is different now.
- The important decision of the Swiss Federal Council.

*Understanding the new regulatory obligations*

- Important Articles of the GDPR.
- The increased importance of information security, international standards, and best practices (Art 2, 4, 5, 9, 10, 25, 30, 32, 35, 40, 45, 47).
  - "Privacy by design" and "privacy by default" (Art. 25 GDPR), "due regard to the state of the art" ((78), (83), Art. 25, Art. 32 GDPR).

*GAP Analysis*

- Performing a data privacy assessment for each department - understanding current business processes that create or use customer data.
- Establishing what must be changed: Enterprise-wide privacy governance structure with clearly defined roles and responsibilities, privacy risks and controls, customer profiling, enterprise-wide personal data retention and destruction, handling customers’ personal data requests, privacy data breaches, data breach response, third parties and outsourcing, data across the borders, privacy training tailored to the employee’s roles and responsibilities.
- Policies, Procedures, Communication, Enforcement. Everybody must understand the new obligations - the Board, the CEO, senior management, and all departments.
Case Studies
- Swiss or non-EU organizations that offer goods or services to EU data subjects via their web site or an online shop.
- Swiss or non-EU organizations that process data in EU countries.
- Swiss or non-EU firms that collect data of EU data subjects’ behaviour for marketing purposes.

Closing
- The Swiss Data Protection Act (DPA) and the “EU-US Safe Harbour” regulation adopted by Switzerland.
- The revised DPA - largely analogical rules and provisions with the GDPR.
- The decisions of the Swiss Federal Data Protection and Information Commissioner (FDPIC).
C11. The General Data Protection Regulation (GDPR) for the Board of Directors and the CEO of Swiss and non-EU based companies

Overview

The GDPR is applicable for Swiss and non-EU companies that are offering goods or services to identified or identifiable EU natural persons ("data subjects"), organizations processing personal data of EU data subjects, or organizations that monitor the online behaviour of EU data subjects. Non-EU companies that have no local presence in the EU are also in scope of the GDPR legislation. Penalties for violating the GDPR could reach € 20 million or 4% of a company’s annual worldwide turnover.

Target Audience:

The program is recommended for:

- The Board of Directors
- The CEO

Duration:

2 hours to half day, depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

Instructor:


Language:

English

The program can include:

- An overview of the GDPR.
- What is different now.
- The important decision of the Swiss Federal Council (it is economically important for Switzerland to be recognized as a country with an appropriate data protection level for the EU).
- Important Articles of the GDPR.
- The increased importance of information security, international standards, and best practices.
- "Privacy by design" and "privacy by default" (Art. 25 GDPR), "due regard to the state of the art" ((78), (83), Art. 25, Art. 32 GDPR).
- Establishing what must be changed: Enterprise-wide privacy governance structure with clearly defined roles and responsibilities, privacy risks and controls, customer profiling, enterprise-wide personal data retention and destruction, handling customers’ personal data requests, privacy data breaches, data breach response, third parties and outsourcing, data across the borders, privacy training tailored to the employee’s roles and responsibilities.
- Policies, Procedures, Communication, Enforcement. Everybody must understand the new obligations - the Board, the CEO, senior management, and all departments.
- The questions every board of directors must ask.
- The Swiss Data Protection Act (DPA) and the “EU-US Safe Harbour” regulation adopted by Switzerland.
- The revised DPA - largely analogical rules and provisions with the GDPR.
- The decisions of the Swiss Federal Data Protection and Information Commissioner (FDPIC).
C12. Certified Risk and Compliance Management Professional (CRCMP), Prep Class Overview

This is a preparation class for the Certified Risk and Compliance Management Professional (CRCMP) program. It has been designed to provide with the knowledge and skills needed to understand and support regulatory compliance and enterprise-wide risk management. The course provides with the skills needed to pass the Certified Risk and Compliance Management Professional (CRCMP) exam.

This is a program developed and provided by the International Association of Risk and Compliance Professionals (IARCP), a business unit of Compliance LLC. George Lekatis, general manager of Cyber Risk GmbH, is also the general manager of Compliance LLC. Cyber Risk GmbH has the permission to organize CRCMP instructor-led training in Switzerland, Liechtenstein, and Germany.

The CRCMP program has become one of the most recognized programs in risk management and compliance. There are CRCMPs in 32 countries around the world.

The CRCMP is a preferred certificate for companies and organizations around the world. For example:
Target Audience

The CRCMP certification program is beneficial to:

- Managers and employees involved in the design and implementation of risk and compliance related strategies, policies, procedures, risk assessments, control activities, testing, documentation, monitoring and reporting.

- Vendors, suppliers, and service providers.

This course is intended for employers demanding qualified professionals that meet the fit and proper requirements.

Duration

One day (09:00-17:00). The instructor will cover the most important and difficult parts of the program, and he will conclude the class with sample questions, that give a good understanding of what is needed for the exam. Each delegate will receive the official presentations of the CRCMP program. After the class, the delegates that want to sit for the CRCMP exam, must spend the
required time to study the presentations and understand the details.

Instructor

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf

Language

English

Course Synopsis

Part A: Introduction, Compliance and Risk Management

What is corporate governance.

The OECD (Organization for Economic Cooperation and Development) principles of corporate governance.

FSB, Thematic Review on Risk Governance.

FSB 2017, Thematic Review on Corporate Governance.

What is risk.

Risk and uncertainty.

Risk acceptance, transfer, avoidance.

Definitions of risk - from the US Marine Corps (Marine Cops Training Command) to the corporate environment.

Risk - good or bad?

Case Study: Daimler Group, Risk and Opportunity Management system.

Risk Management and Issue Management.

Marine Corps and Banks – similar Records Management principles.

Threats and vulnerabilities.

Risk mitigation methodology flowchart.

Outsourcing and Risk Management.

What is compliance.

Enterprise wide risk and compliance program.

Case Study: Annual Report, Munich Re.

Policies, Procedures, Standards, Baselines, Guidelines, Ethics.
Case Study: Merck.
Conflicts of interest.
Roles and responsibilities.
The Chief Risk Officer.

Case Study: Annual Report, Bank of America Corporation.
Case Study: Annual Report, Credit Suisse Group AG.
Case Study: Annual Report, Munich Re.

Data Owners, Process Owners.
The role of the internal auditors.
Continuous Auditing.
The role of the external auditors.
The role of the Board of Directors.
Case Study: Annual Report, Credit Suisse Group AG.
Case Study: Annual Report, GE.
Case Study: Annual Report, Lloyds Banking Group.
Case Study: Annual Report, Bank of America.
Case Study: Annual Report, Amazon.
Case Study: Annual Report, Daimler Group.

**Part B: Sarbanes-Oxley, an international standard.**
The need.
Companies affected.
American Depository Receipt (ADR) program.
Employees affected.
Foreign Private Issuers (FPIs) and Sarbanes-Oxley compliance.
EDGAR - Electronic Data Gathering, Analysis, and Retrieval system.
Case Studies: Microsoft, Sony.

The Sarbanes-Oxley Act.
Key sections, what we need to know.
Board's new responsibilities.
Management’s testing and documentation.
Management’s responsibilities.
Committees and teams.
Sections 302, 404, 906: The three certifications.
Sections 302, 404, 906: Examples and case studies.

The Securities and Exchange Commission (SEC) and the Sarbanes-Oxley Act.
The PCAOB and the new Auditing Standards: What we need to know.
Auditing Standard No. 1, to Auditing Standard No. 16.
Reorganized PCAOB Auditing Standards.

Control Deficiency.
Deficiency in Design.
Deficiency in Operation.
Significant Deficiency.
Material Weakness.

The Scope of the Sarbanes-Oxley Act.
Software and Spreadsheets after the Sarbanes-Oxley Act.
Service providers.

E-SOX, the European Sarbanes-Oxley.
The 8th Company Law Directive of the European Union.
Ahold, Parmalat and the new rules.
Article 45 - Registration and oversight of third-country auditors and audit entities.
The “equivalence” of a third country.
Article 46 - Derogation in the case of equivalence.

J-SOX, the Japanese Sarbanes-Oxley.
From Enron to Livedoor, Kokudo, Kanebo.
The Financial Instruments and Exchange Law.
J-SOX requirements similar to the U.S. Sarbanes-Oxley Act.
“Corporate Responsibility for Financial Reports”
“Management Assessment of Internal Controls”
From the Financial Services Agency (FSA), to the Certified Public Accountants and Auditing Oversight Board (CPAAOB), to the Securities and Exchange Surveillance Commission (SESC).
Part C: Basel II, Basel III – the new international standards in governance, risk and compliance

The Bretton Woods Agreement.

Bankhaus Herstatt.

The Bank for International Settlements (BIS).

The Basel Committee on Banking Supervision (BCBS).

The purposes of the Basel framework.

Basel I, Basel II, Basel III.

Basel I - The First Basel Capital Accord.

Basel II - The major amendment.

Pillar 1: Minimum capital requirements.

Pillar 2: Supervisory review process.

Pillar 3: Market discipline.

Branch office vs. subsidiary.

Credit risk, market risk, operation risk.

Operating, Operations, Operational risks.

Seven Event Types (Loss Categories).

The 8 business lines.

Delphi method - exploring the future.

5 categories of control breakdowns.

Outsourcing and Basel compliance.

The Basel III amendment.

The objective of the reform.

Basel III, sound corporate governance principles.

A. Board practices.

B. Senior management.

C. Risk management and internal controls.

D. Compensation.

E. Complex or opaque corporate structures.

F. Disclosure and transparency.

The role of the supervisors.

Part D: The Frameworks
The Committee of Sponsoring Organizations (COSO).


The COSO cube.

Control Environment.
Risk Assessment.
Control Activities.
Information and Communication.
Monitoring.

Effectiveness and Efficiency of Operations.
Compliance with applicable laws and regulations.

2013, COSO Internal Control — Integrated Framework.

The updated COSO cube.

Example: Cyber risk and COSO.

2004 - The COSO Enterprise Risk Management (ERM) Framework.

The differences between COSO and COSO ERM.

Components of Enterprise Risk Management.

The COSO ERM cube.

Is COSO ERM needed for compliance?

Internal Environment.
Objective Setting.
Event Identification.
Risk Assessment.
Risk Response.
Control Activities.
Information and Communication.
Monitoring.

Objectives: Strategic, Operations, Reporting, Compliance.

ERM – Application Techniques.

2017 - The updated COSO ERM.
Enterprise Risk Management and Strategy Selection.

Control Objectives for IT - COBIT.
COBIT 5.

*Part E: Designing and implementing a risk and compliance program*

Which is the best program?
Principles of Effective Compliance Programs, from the US Bureau of Industry and Security.
Comprehensive compliance programs.

The Rulemaking Process in the US and the EU.
International and national regulatory requirements.
C13. Certified Information Systems Risk and Compliance Professional (CISRCP), Prep Class

Overview
The seminar has been designed to provide with the knowledge and skills needed to understand the legal and regulatory obligations that shape international standards and best practices in risk, compliance, IT, information security and privacy protection, and to become a Certified Information Systems Risk and Compliance Professional (CISRCP).

The program has been developed and provided by the International Association of Risk and Compliance Professionals (IARCP), a business unit of Compliance LLC. George Lekatis, general manager of Cyber Risk GmbH, is also the general manager of Compliance LLC. Cyber Risk GmbH has the permission to organize CISRCP instructor-led training in Switzerland, Liechtenstein, and Germany.

Companies and organizations must always rely on expert opinion and technical advice that is based on laws and regulations. To minimize liability and reduce risks, including losses from legal action, managers and experts must understand the current legal environment.

The CISRCP program deals with the interaction of US and EU executive orders, directives and
regulations that shape international standards and best practices. It covers the General Data Protection Regulation (GDPR) of the EU, and the extraterritorial application of EU law, including the data protection “by design” and “by default”.

**Objectives:**

**Target Audience**
The CISRCP certification program is beneficial to:

- Managers and employees involved in the design and implementation of risk, compliance, IT, information security and privacy protection strategies, policies, procedures, risk assessments, control activities, testing, documentation, monitoring and reporting.
- Vendors, suppliers and service providers.

This course is intended for employers demanding qualified professionals that meet the fit and proper requirements.

**Duration**
One day (09:00-17:00). The instructor will cover the most important and difficult parts of the program, and he will conclude the class with sample questions, that give a good understanding of what is needed for the exam. Each delegate will receive the official presentations of the CISRCP program. After the class, the delegates that want to sit for the CISRCP exam, must spend the required time to study the presentations and understand the details.

**Instructor**
Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Language**

English

**Course Synopsis**

*Part 1: US Executive Orders and federal government regulation that shape cybercrime laws, regulations and international standards.*

Executive orders.


The National Strategy to Secure Cyberspace.

Einstein 1, 2, E3A.
Executive Order 13587.
Executive Order (EO) 13636.
PPD 21.
Executive Order 13636.
Executive Order 13691.
PPD 41.
Executive Order 13794.
Executive Order 13800.

US federal government regulation.
Health Insurance Portability and Accountability Act (HIPAA).
Gramm-Leach-Bliley Act.

Part 2: The European Union's directives and regulations that shape international standards.
Directive 2013/40/EU.

The European Agenda on Security, 2015.

The EU Computer Emergency Response Team (CERT-EU).
Europol’s Cybercrime Centre (EC3).
The EC3 Programme Board.

The directive on security of network and information systems (NIS Directive), 2016.
The NIS Directive, important parts.

Critical infrastructure protection in the EU.
Directive 2008/114/EC.
JOIN (2017) 450.
Reform of cyber security in Europe.
Part 3: The General Data Protection Regulation (GDPR) of the EU, and the extraterritorial application of EU law.

Important sections of the GDPR.
Principles relating to processing of personal data.
Data protection "by design" and "by default".
Representatives of controllers or processors not established in the Union.
Information security.
Security of processing.
Appropriate level of security, "taking into account the state of the art".
The "data protection impact assessment ".
Transfers of personal data to third countries.
GDPR practical steps, from ENISA.

Closing remarks.
World Economic Forum, Global Centre for Cybersecurity.
C14. Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, Prep Class

Overview

This program has been designed to provide with the knowledge and skills needed to support firms and organizations in Cyber Governance, Risk, and Compliance Management. The course also provides with the skills needed to pass the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P exam.

The program has been developed and provided by the International Association of Risk and Compliance Professionals (IARCP), a business unit of Compliance LLC. George Lekatis, general manager of Cyber Risk GmbH, is also the general manager of Compliance LLC. Cyber Risk GmbH has the permission to organize CISRCP instructor-led training in Switzerland, Liechtenstein, and Germany.

Target Audience

The CC(GRC)P certification program is beneficial to:

- Managers and employees working at the strategic, tactical, and operational levels of information security, IT, risk, and compliance management.
- Information security managers, employees, auditors, and consultants.
- Threat analysts.
- Vulnerability assessment managers, employees, auditors, and consultants.
- Data protection and privacy managers, employees, auditors, and consultants.
- Vendors, suppliers, and service providers.

This course is intended for employers demanding qualified cyber security and privacy professionals that meet the fit and proper requirements in risk and compliance management.

**Duration**

One day (09:00-17:00). The instructor will cover the most important and difficult parts of the program, and he will conclude the class with sample questions, that give a good understanding of what is needed for the exam. Each delegate will receive the official presentations of the CC(GRC)P program. After the class, the delegates that want to sit for the CC(GRC)P exam, must spend the required time to study the presentations and understand the details.

**Instructor**

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: [www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf](http://www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf)

**Language**

English

**Course Synopsis**

**Part 1: Introduction**

- Demand for Cyber Risk / Information Security Professionals ... and compensation.
- Introduction to Cyber (Governance, Risk, Compliance).
- From Cyberspace to Information Operations (IO) to Cyber Espionage.
- Cyber risks today, and what is different for organizations and employees.

**Part 2: Attacks and Modus Operandi**

- Who is the attacker?
- Eleven types of internet security attacks.
- 1. Attacks on the critical infrastructure.
- 3. Deliberate persistent attacks on specific resources.
- 4. Widespread automated attacks against internet sites.
- 5. Threats, harassment, and other criminal offences involving individual user accounts.
- 6. New types of attacks or new vulnerabilities.
- 8. Denial of Service (DoS) and Distributed Denial of Service (DDoS).
- 10. Compromise of single desktop systems.
- 11. Copyright violations.

Modus Operandi

Step 1 - Collecting information about persons and systems
- Reconnaissance: The research phase used to identify and select targets.
- Looking for information about the systems.
- Looking for information about the persons working in the target organization (or for the target organization).
- Outsourcing and budget cuts can have hidden costs.
- Who has signed a confidentiality agreement? A good list of prime targets for all adversaries.
- Looking at our daily activities from the adversaries' point of view.
- More prime targets: Disgruntled employees, ideologists, employees having a lavish lifestyle, employees having “weaknesses”, lawyers having access to trade secrets and sensitive information.

Step 2 - Identifying possible targets and victims
- Hardware attacks, software attacks.
- Malicious hardware modifications: Acquiring hardware components with a backdoor, and how it affects all other information security policies.
- Phishing, social phishing, spear phishing, watering hole attacks.
- Which systems and which persons? The hit list.

Step 3 - Evaluation, recruitment, and testing
- Exploiting more vulnerabilities in certain systems.
- Deciding to work more with certain persons.
- Blackmailing employees: The art and the science.
- Testing the asset.
- The problem with the sleeper agents.

Step 4 - Privilege escalation
- A. Vertical privilege escalation, where adversaries grant themselves higher privileges.
- B. Horizontal privilege escalation, where adversaries use the identity of other users with similar privileges.
- Obtaining customer account details.
- Internal information, social engineering.
**Step 5 - Identification of important clients and stakeholders**
- Attackers have access to personal information. What is next?
- Identifying important clients and stakeholders working in the public and the private sector.
- Repeating the process - Steps 1 to 4.

**Step 6 - Critical infrastructure**
- Creating backdoors.
- Covering their tracks.
- Ticking time bombs and backdoor triggers based on specific input data.
- Selling information in the secondary markets (to other attackers, competitors, spies, and the organized crime).
- The deep web.
- The dark web.
- Examples and case studies.

**Part 3: Information Warfare, Cyber Espionage**

**Information Warfare**
- The famous paradoxical trinity of Clausewitz.
- Cyberspace – a domain of war.
- Jus ad bellum, jus in bello, jus post bellum.
- Article 2(4) and Article 51, United Nations (UN) Charter.
- Interpretations of Article 2(4) and Article 51.
- Information Operations (IO).
  - 1. Electronic warfare (EW).
  - 2. Computer network operations (CNO).
  - 3. Psychological operations (PSYOP).
  - 4. Military deception (MILDEC), and
  - 5. Operations security (OPSEC).
- Information Operations and their supporting capabilities.
  - 1. Information Assurance.
  - 4. Counter Intelligence.
  - 5. Combat Camera.
- Defensive Information Operations.
- Net-centric warfare.
- Cyberspace and national security.
- Hackers, Spies, or Hybrid Warfare?
- The Gerasimov’s Doctrine.
- Case Studies.

**Cyber Espionage.**
- Espionage, Intelligence.
- Political, Economic, Military Intelligence.
- Competitive Intelligence vs. Economic or Industrial Espionage.
- From UK, MI5.
- From UK SIS, MI6.
- From UK, Centre for the Protection of National Infrastructure (CPNI).
- Counterintelligence (CI).
- Cyber Espionage.
- Case studies.
- Strategic counterintelligence.
- The Ten Commandments of Counterintelligence (from James M. Olson that served in the Directorate of Operations of the CIA) that apply in Cybersecurity.
- Gentlemen don’t read each other’s mail?

**Part 4: Defense**
- Cyber Hygiene.
- The U.S. National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
  - 1. The Framework Core.
  - 3. The Framework Profile.
- The Functions:
  - a. Identify.
  - b. Protect.
  - c. Detect.
  - d. Respond.
  - e. Recover.
- From ID.AM-1: Physical devices and systems within the organization are inventoried, to ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
- From ID.BE-1: The organization’s role in the supply chain is identified and communicated, to ID.BE-5: Resilience requirements to support delivery of critical services are established.
- From ID.GV-1: Organizational information security policy is established, to ID.GV-4:
Governance and risk management processes address cybersecurity risks.
- From ID.RA-1: Asset vulnerabilities are identified and documented, to ID.RA-6: Risk responses are identified and prioritized.
- From ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders, to ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.
- From PR.AC-1: Identities and credentials are managed for authorized devices and users, to PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.
- From PR.AT-1: All users are informed and trained, to PR.AT-5: Physical and information security personnel understand roles & responsibilities.
- From PR.DS-1: Data-at-rest is protected, to PR.DS-7: The development and testing environment(s) are separate from the production environment.
- From PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, to PR.IP-12: A vulnerability management plan is developed and implemented.
- From PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools, to PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
- From PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy, to PR.PT-4: Communications and control networks are protected.
- From DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed, to DE.AE-5: Incident alert thresholds are established.
- From DE.CM-1: The network is monitored to detect potential cybersecurity events, to DE.CM-8: Vulnerability scans are performed.
- From DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability, to DE.DP-5: Detection processes are continuously improved.
- RS.RP-1: Response plan is executed during or after an event.
- From RS.CO-1: Personnel know their roles and order of operations when a response is needed, to RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
- From RS.AN-1: Notifications from detection systems are investigated, to RS.AN-4: Incidents are categorized consistent with response plans.
- From RS.MI-1: Incidents are contained, to RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
- From RS.IM-1: Response plans incorporate lessons learned, to RS.IM-2: Response strategies are updated.
- RC.RP-1: Recovery plan is executed during or after an event.
- From RC.IM-1: Recovery plans incorporate lessons learned, to RC.IM-2: Recovery strategies are updated.
- From RC.CO-1: Public relations are managed, to RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams.
- The Framework Implementation Tiers (“Tiers”).
- From Partial (Tier 1) to Adaptive (Tier 4).
- The Framework Profile.
- Coordination of Framework Implementation.
- Establishing or Improving a Cybersecurity Program.
- Step 1: Prioritize and Scope.
- Step 2: Orient.
- Step 3: Create a Current Profile.
- Step 4: Conduct a Risk Assessment.
- Step 5: Create a Target Profile.
- Step 6: Determine, Analyze, and Prioritize Gaps.
- Step 7: Implement Action Plan.
- Methodology to Protect Privacy and Civil Liberties.
- Governance of cybersecurity risk.
- Awareness and training measures.
- Penetration Testing.
- Guidance from the Securities and Exchange Commission (SEC), Division of Corporation Finance, regarding disclosure obligations relating to cybersecurity risks and cyber incidents.
- The new international standards for cyber security after Regulation (EU) 2016/679 (General Data Protection Regulation).

**Part 5: The future**
- The attribution problem.
- The second attribution problem.
- Plausible deniability.
- Misinformation, disinformation, deception, fabrication.
- Disinformation management.
- ENISA, Disinformation operations in cyber-space.
- ENISA, Active Defense and Offensive Countermeasures.
C15. Information Security Awareness Training

Overview

There is no successful information security program without an effective information security awareness training program for all managers and employees of a company or an organization, that are usually the weakest link in information security.

If managers and employees do not understand the risks and the consequences, it is unlikely to comply with corporate policies. They will continue to cut corners and compromise security in the name of convenience.

Process owners and persons having access to systems and data must understand the cyber security threats, and they must learn what they can do to protect themselves, their firm or organization, and the critical infrastructure.

Target Audience

The program is beneficial to all managers and employees of companies and organizations of the private and the public sector.
Duration
Half day (09:00-13:00) to one day (09:00-17:00), depending on the needs, the content of the program and the case studies. We always tailor the program to the needs of each client.

Instructor
Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: www.cyber-risk-gmbh.com/George_Lekatis_Testimonials.pdf

Language
English

Course Synopsis:

Understanding the importance of information security
- Legal and regulatory obligations.
- Importance of information security for the organization and the country.
- Importance of information security for the employees and contractors.

Desktop Security
- A password-protected screen saver.
- Locking computers when users walk away from them.
- Shoulder surfing.
- Key loggers.

Password Security
- Eliminating default passwords.
- What constitutes a strong, secure passphrase.
- Cracking passwords.
- Minimum password requirements.
- Sharing passwords.
- Examples of passphrases.

Wireless Security
- The ease of use vs. security.
- The wireless networks and possible security problems.
- Mobile Devices and Wireless.

**Email Security**
- Protecting information when using the internet and email.

**Malware**
- Viruses, worms, trojans, spyware, adware.
- Examples and case studies.

**Phishing**
- What is phishing.
- Examples and case studies.
- Things to avoid.
- Clicking on links provided in e-mails.

**Social engineering, hoaxes, scams**
- Social engineering examples and case studies.
- Types of hoaxes.
- Examples and case studies.
- Comparing hoaxes to viruses.
- Preventing the spread of hoaxes.
- Social Engineering.

**Social Media**
- Risks to the person and the organization.
- Exploiting human networks.

**Legal issues**
- File sharing and copyright.
- Downloading unknown or unsolicited programs or files.
- Copyrighted documents in the corporate network.
- Recordings, videos, software.
- Illegal file sharing and downloading.

**Travel Security**
- Laptops.
- Corporate data and intellectual property.
- Examples and case studies.

*Reporting security incidents*

- The importance of reporting, from policies to reality.

*Closing*

- Examples and case studies. Closing remarks.
C16. Your program

Overview

Let us know what you have in mind. We can develop and tailor the program to meet your requirements. You may contact us to discuss your needs.

Duration:

To be decided.

Instructor

Our instructors are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

George Lekatis can also lead the class. His background and some testimonials can be found at: 

Language:

English.
Cost, terms and conditions, cancellation policy for on-site instructor-led training

Cost

Unless otherwise agreed, the training services shall be provided at a fixed price, plus VAT and reasonable travelling expenses and allowances that will be pre-approved by the client. The client will be provided with timesheets and breakdowns of time spent and expenses. Payments shall only be made against an invoice.

For one day (09:00-17:00) in-house instructor-led training, delivered at the client’s premises, the cost is CHF 6’000 (plus VAT and reasonable travelling expenses and allowances) for 1-20 participants, and CHF 200 (plus VAT) for each additional participant (over 20 participants).

For 1 hour to half day in-house instructor-led training, delivered at the client’s premises, the cost is CHF 4’000 (plus VAT and reasonable travelling expenses and allowances) for 1-20 participants, and CHF 100 (plus VAT) for each additional participant (over 20 participants).

In-House Instructor-Led Terms and Conditions, Cancellation Policy:

a. 50% of the cost of each training program (including 50% of the total estimated expenses) is billable in advance and is payable 15 days prior to the course delivery date. The remaining 50% of the cost (including the remaining expenses) is due 30 days after the last day of the training.

b. Cancellation from the client less than 15 days before the scheduled start date will be subject to a
cancellation fee of CHF 2'500.
Cancellation from the client 15-29 days before the scheduled start date will be subject to a
cancellation fee of CHF 1'600.
Cancellation from the client 30 days or more before the scheduled start date will not be subject to
any cancellation fee.
c. Force Majeure - Neither the client nor Cyber Risk GmbH shall be liable to any penalty should
courses be cancelled due to war, fire, strike lock-out, industrial action, accident / illness of the
instructor, civil disturbance, or any other cause whatsoever beyond their control.
d. In the unlikely event of a cancellation by Cyber Risk GmbH, any payment made for the
cancelled class or presentation will be refunded. The client understands and agrees that Cyber
Risk GmbH shall not, in any way, be held responsible for any costs, including loss of airfare or
other transportation costs, hotel expenses or other damages, which the client may suffer if Cyber
Risk GmbH cancels a class.
e. Cyber Risk GmbH processes and stores data in compliance with both, the Swiss Federal Act on
Data Protection (FADP) and the EU General Data Protection Regulation (GDPR). The service
provider is Hostpoint (the servers are in the interxion data center in Zurich, the data is saved
exclusively in Switzerland, and support, development and administration activities are also based
entirely in Switzerland).
f. Cyber Risk GmbH will neither take any photos of the audience, nor publish any names, photos,
or details of the training agreement on social media, web sites or catalogs, for marketing or for any
other purpose.
g. The copyright and all intellectual property rights relating to the training material provided to
the client are solely owned by and hereby reserved to Cyber Risk GmbH. Under no circumstances
may the whole or any part of the training material be produced or copied in any form or by any
means or translated into another language without the prior written permission of Cyber Risk
GmbH.
h. Cyber Risk GmbH is willing to sign a confidentiality or nondisclosure agreement, shall maintain
confidential information in trust and confidence, and shall not disclose or use confidential
information for any unauthorized purpose. Cyber Risk GmbH may use confidential information of
the client only to the extent required to accomplish the purposes of the training program.
D1. Cyber and Privacy Needs Assessment
A needs assessment is a systematic exploration of the way things are, and the way they should be. The key is to seek the gap between the current situation and the desired situation.
We investigate which are the cyber risk and privacy requirements for your organization. Do you need to comply with the Swiss, the EU, or the US requirements, or all these requirements together? What about the standards at the level of the group?
We compare your existing standards with the required standards.
We develop a confidential report explaining what we have found.
We give a presentation to the Board of Directors, the CEO and the CRO and we answer all questions.

D2. Cyber and Privacy Risk Assessment
We learn which are your cyber risk and privacy standards, policies, procedures, and code of ethics.
We examine which is the actual performance of employees, suppliers, service providers and all stakeholders. Do they meet the Board’s expectations?
We develop a confidential report explaining what we have found.
We give a presentation to the Board of Directors, the CEO and the CRO and we answer all questions.

Cost
You may contact us.
E. Contact us

Cyber Risk GmbH
Rebackerstrasse 7
8810 Horgen
Tel: +41 43 810 43 61
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341.

We process and store data in compliance with both, the Swiss Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR). The service provider is Hostpoint (the servers are in the interxion data center in Zurich, the data is saved exclusively in Switzerland, and support, development and administration activities are also based entirely in Switzerland).