

Cyberrisques et threat intelligence

Breakout Session – Symposium des petites banques du 14 janvier 2019

14 janvier 2019

Ordre du jour

- **Cyberrisques**
 - Qu'entend la FINMA par cyberrisques ?
 - Comment la réglementation est-elle structurée ?
- **Threat intelligence**
 - Présentation du concept
 - Aspects essentiels : menaces, points faibles, « crown jewels »
 - Appréciation de l'auto-évaluation pour les banques des catégories 2 et 3
- **CEO Fraud**
 - Exemple pratique
 - *Lessons learned*

Cyberriques

Yves Obrist

Qu'entend la FINMA par cyberrisques ?

Définition des « cyberattaques » selon la circ.-FINMA 08/21 « Risques opérationnels – Banques », **note de bas de page 20** :

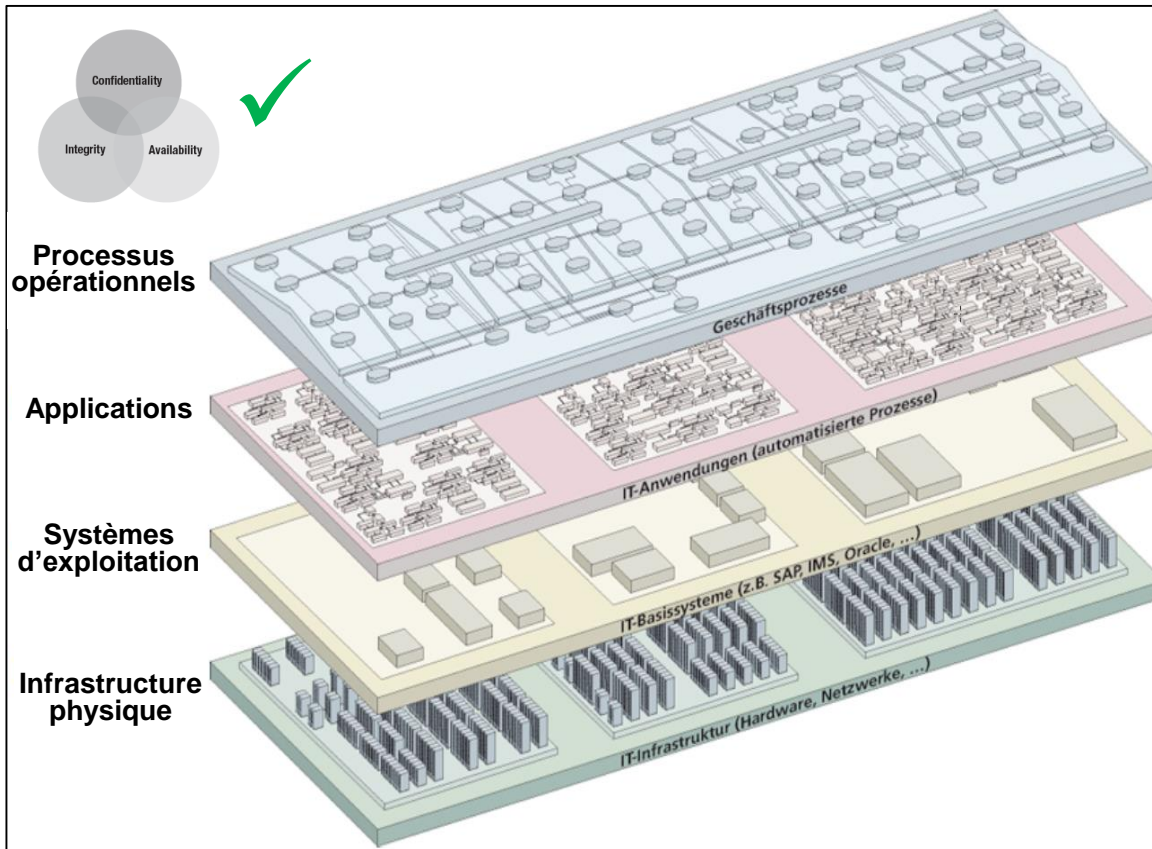
Il s'agit d'attaques en provenance d'**Internet** et de **réseaux comparables** qui visent l'**intégrité**, la **disponibilité** et la **confidentialité** de l'**infrastructure technologique**, notamment en ce qui concerne les **données et systèmes IT critiques et/ou sensibles**.



La **confidentialité** implique la protection contre tout accès non autorisé, tandis que l'**intégrité** recouvre la protection contre toute modification non autorisée et la **disponibilité** la protection contre les interruptions de l'accès.

Qu'entend la FINMA par cyberrisques ?

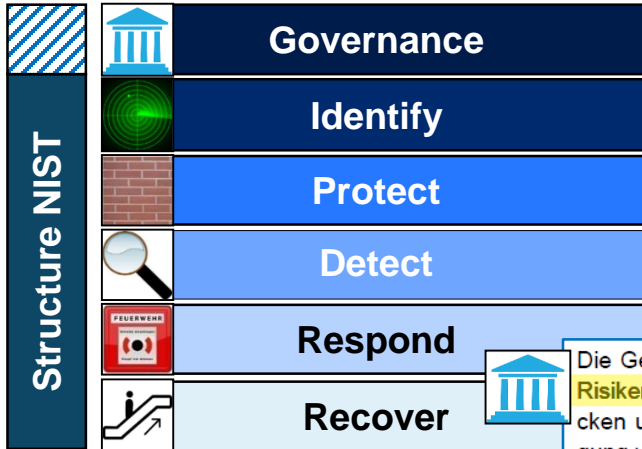
Définition de « l'infrastructure technologique » selon circ.-FINMA 08/21 « Risques opérationnels – Banques », **note de bas de page 17** :




L'**infrastructure technologique** désigne la **structure** (électronique) **physique et logique** des systèmes IT et de communication, les différentes composantes matérielles et logicielles, les données et l'environnement d'exploitation.


Source : ISACA Chapter Suisse


Comment la réglementation est-elle structurée?





Circ.-FINMA 2008/21 « Risques opérationnels – Banques »


- 


Die Geschäftsleitung hat zudem ein **Risikomanagement-Konzept für den Umgang mit Cyber-Risiken**¹⁷ zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch **geeignete Prozesse** sowie eine eindeutige Festlegung von **Aufgaben, Rollen und Verantwortlichkeiten** zu gewährleisten: 135.6*
- 

Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacks¹⁹, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme, 135.7*
- 

Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacks, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IT-Systeme, 135.8*
- 

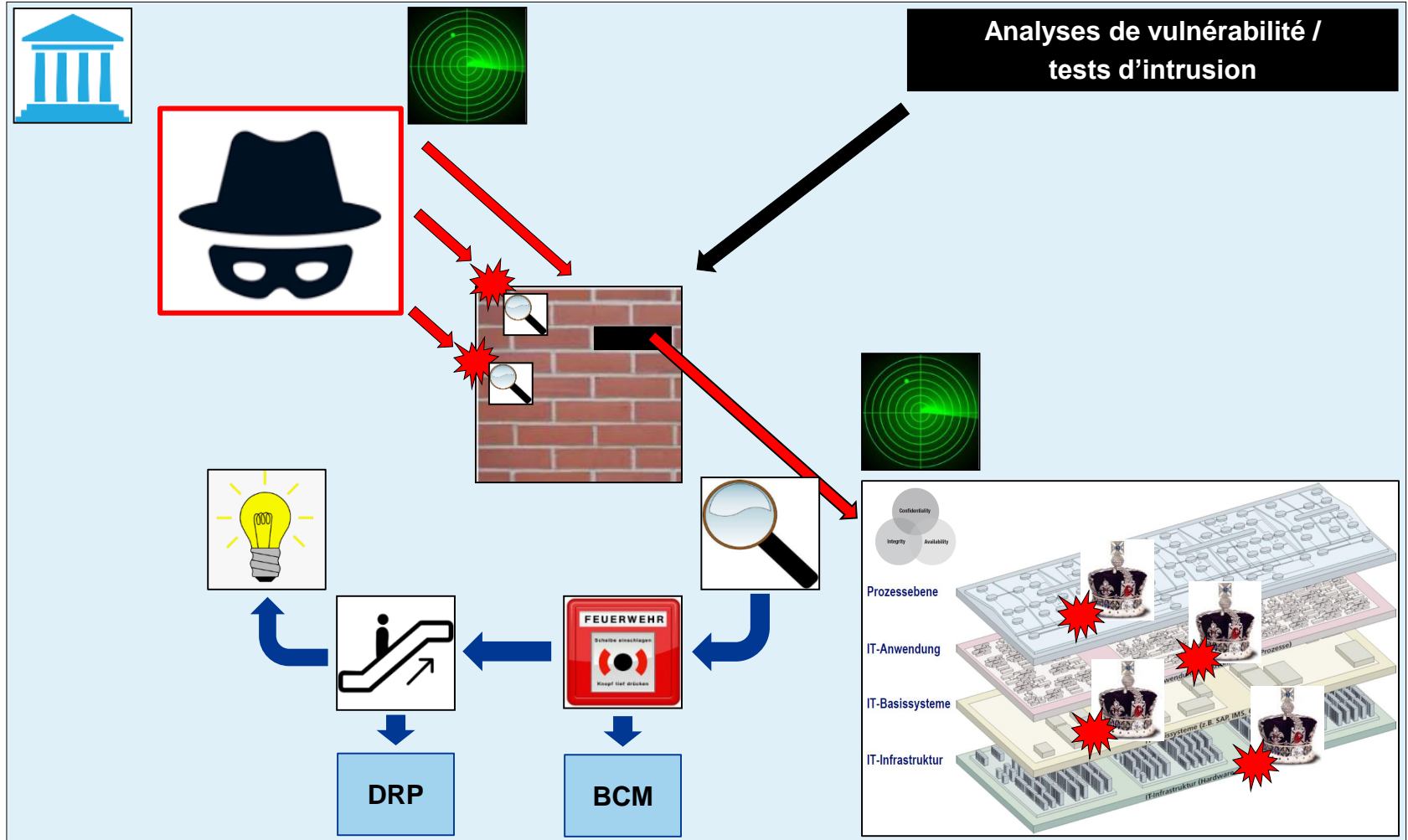
Zeitnahe **Erkennung** und Aufzeichnung von Cyber-Attacks auf Basis eines Prozesses zur systematischen Überwachung der Technologieinfrastruktur, 135.9*
- 

Reaktion auf Cyber-Attacks durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacks in Abstimmung mit dem BCM, und 135.10*
- 

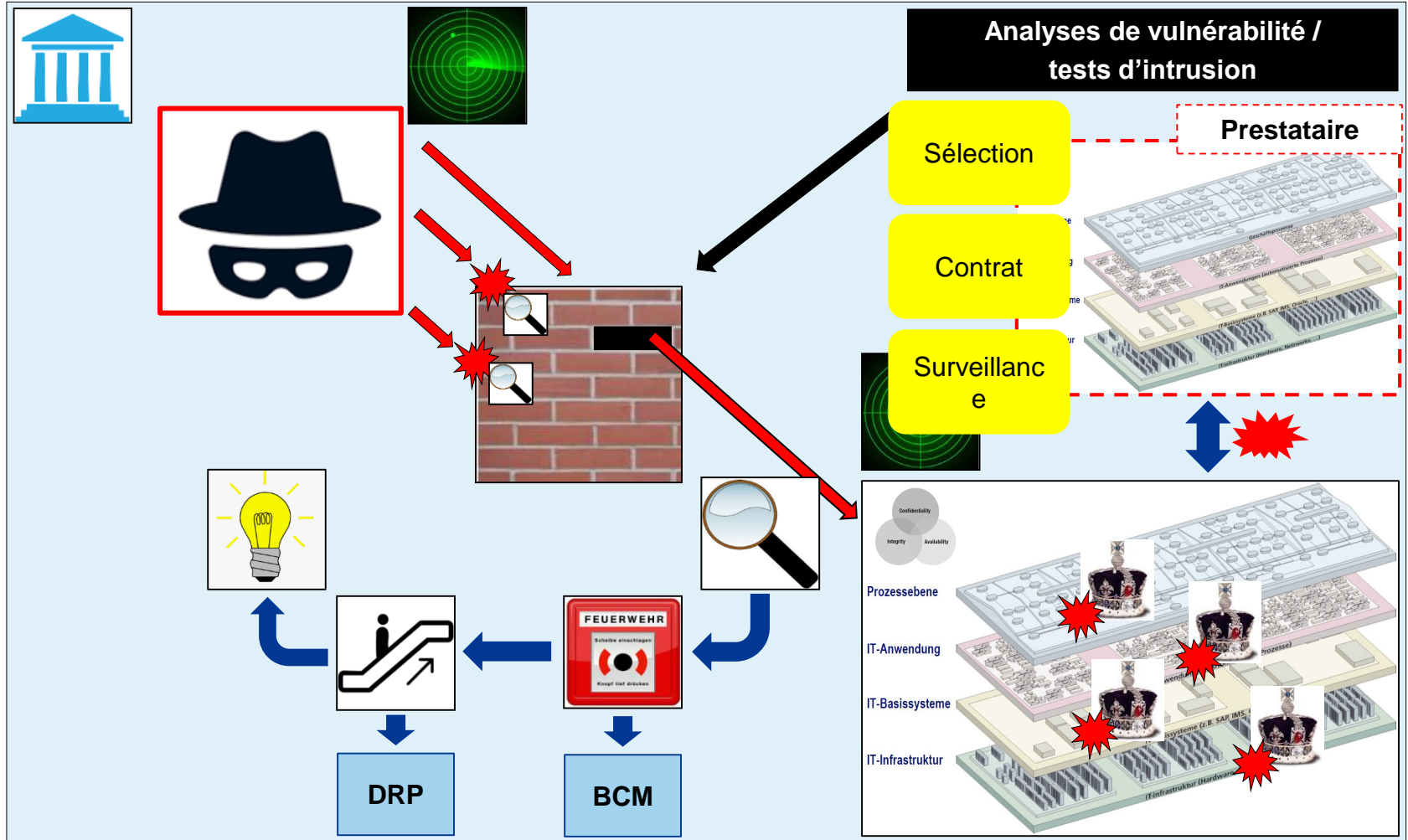
Sicherstellung einer zeitnahen **Wiederherstellung** des normalen Geschäftsbetriebs nach Cyber-Attacks durch geeignete Massnahmen. 135.11*
- 

Die Geschäftsleitung lässt zum Schutz der kritischen und/oder sensitiven Daten und IT-Systemen vor Cyber-Attacks regelmässig **Verwundbarkeitsanalysen**²⁰ und **Penetration Testings**²¹ durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen durchgeführt werden. 135.12*

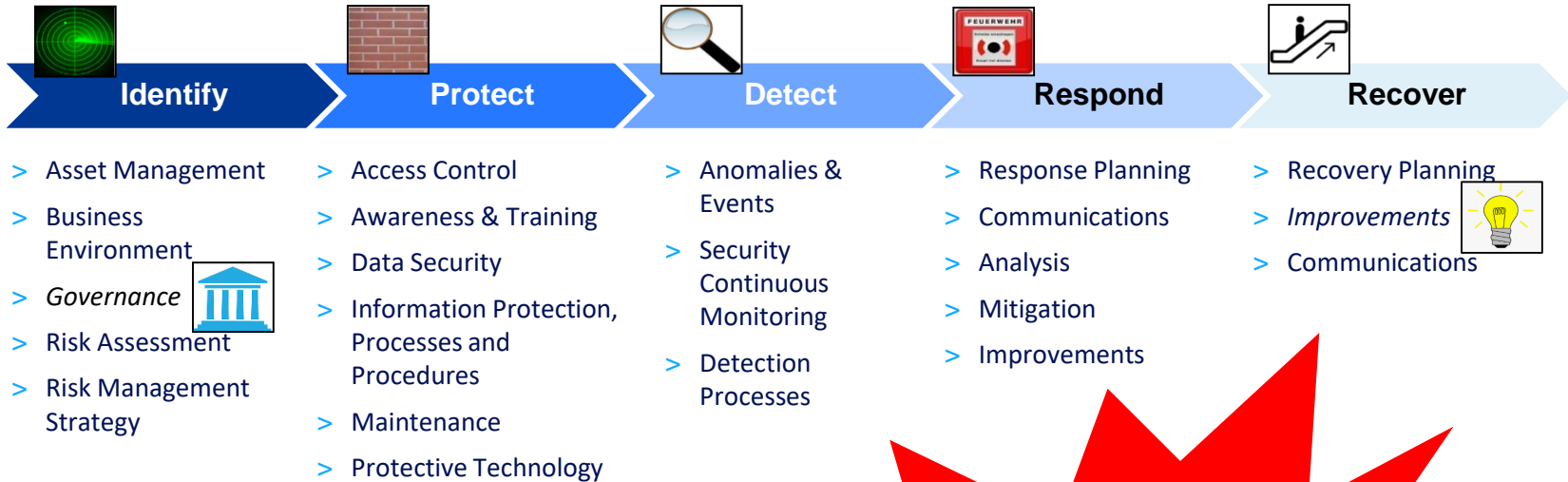
Comment la réglementation est-elle structurée?



Comment la réglementation est-elle structurée?

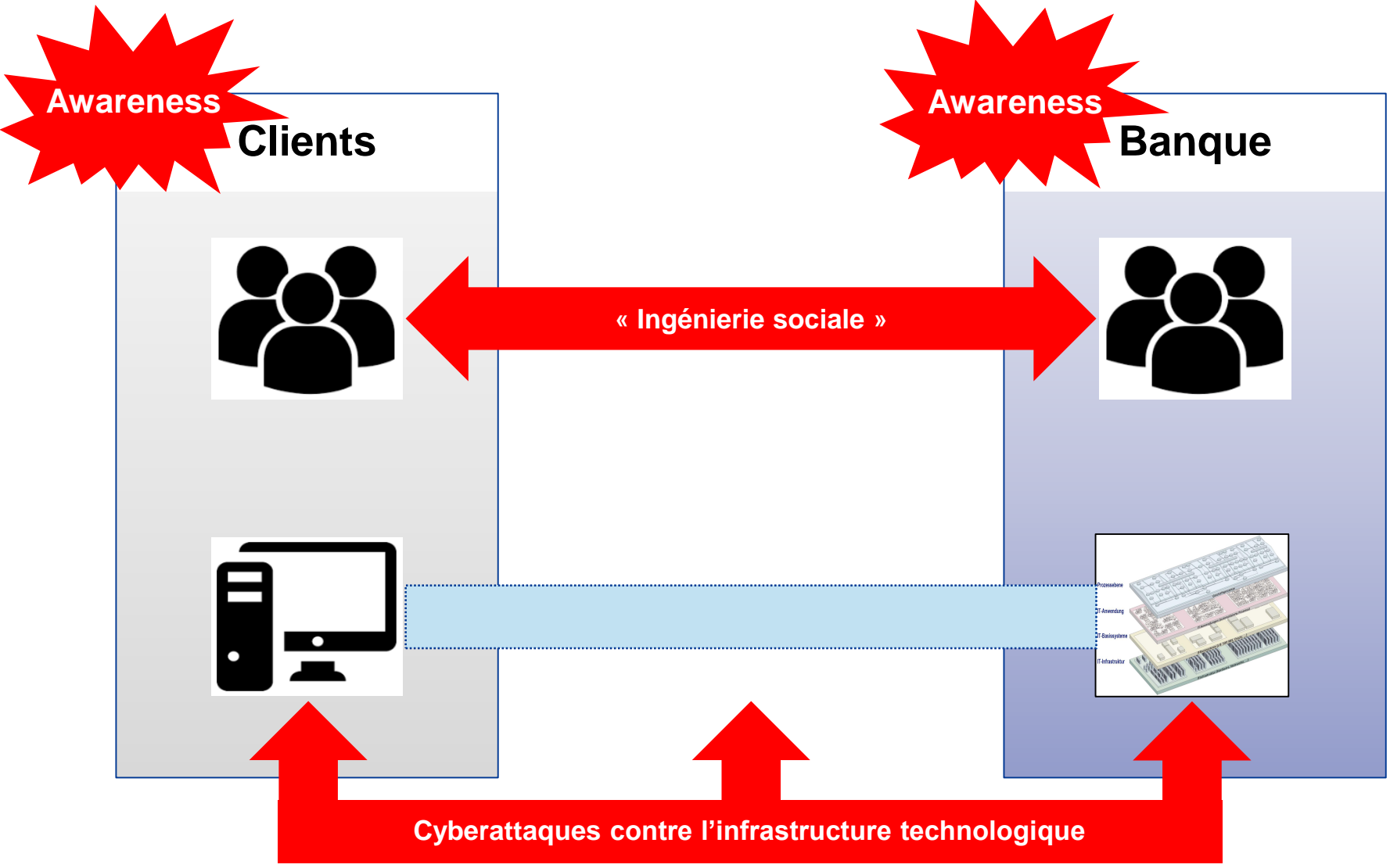


Comment la réglementation est-elle structurée?

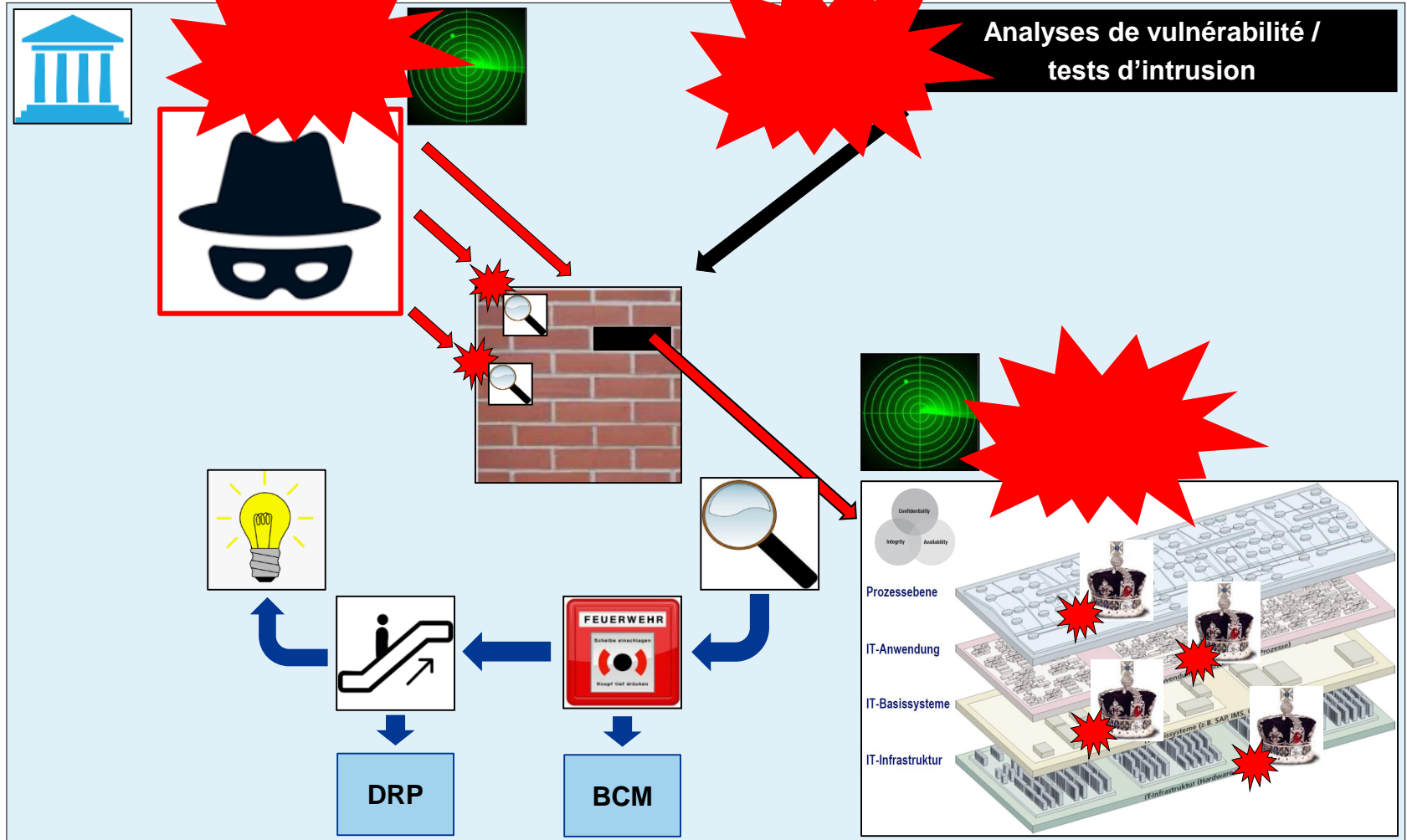


Application du principe de proportionnalité

Favoriser la prise de conscience!



Cyberrisques → Threat Intelligence



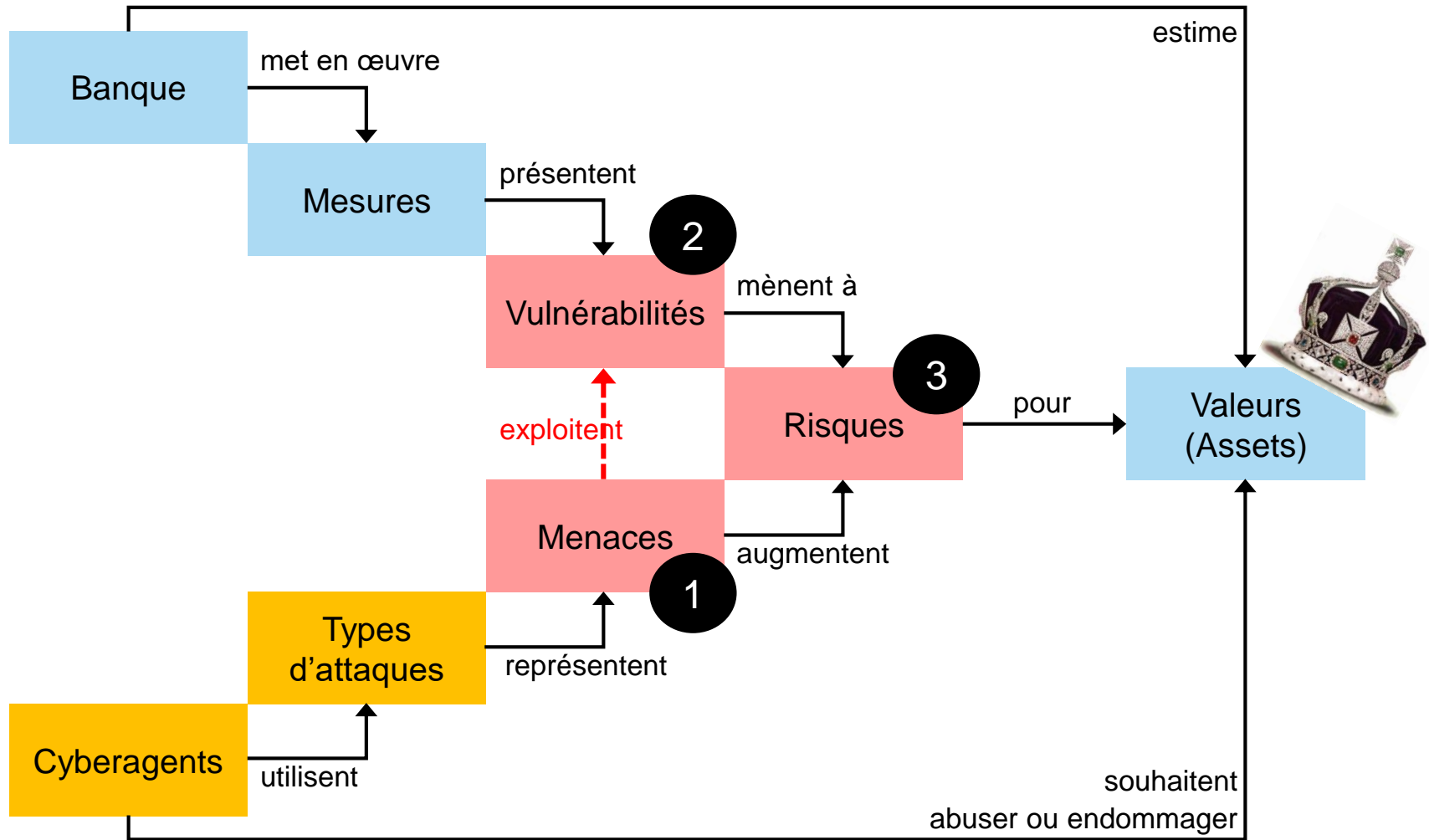
Threat intelligence

Christian Steffen

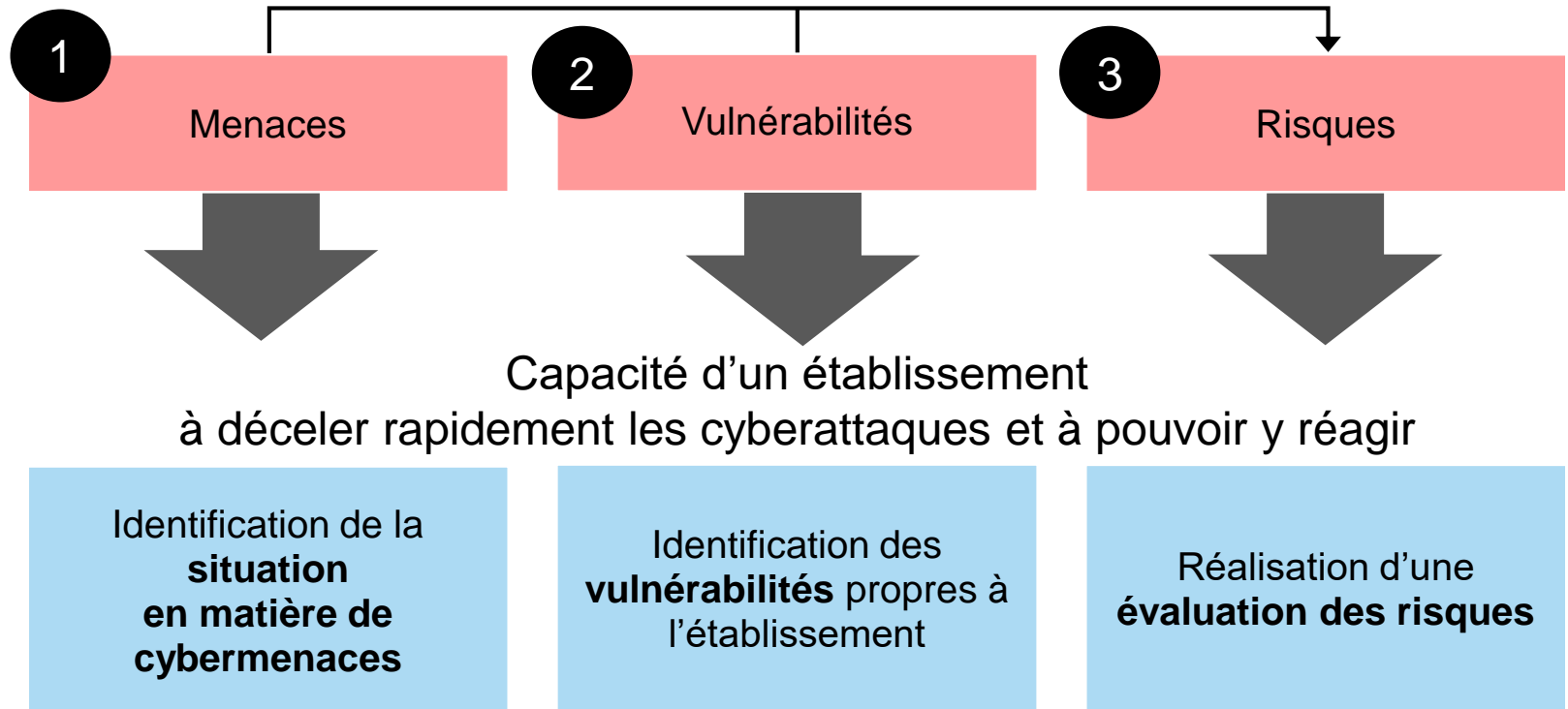
Auto-évaluation 2018

- La FINMA considère la « threat intelligence » comme **cruciale** pour **repousser efficacement** les cyberattaques.
- A l'été 2018, la FINMA a invité **les banques des cat. 2 et 3** à participer à une **auto-évaluation** sur le traitement de la « threat intelligence » (*participation : 3 banques de la catégorie 2 et 23 de la catégorie 3*).
- Dans le cadre du **droit de la surveillance**, le traitement de la « threat intelligence » repose sur le principe 4 « Infrastructure technologique » de la **Circ.-FINMA 2008/21** « Risques opérationnels – banques ».
- Les aspects abordés dans le questionnaire ne sont en général pas des exigences prudentielles explicites. La FINMA les considère cependant comme des **bonnes pratiques** importantes.

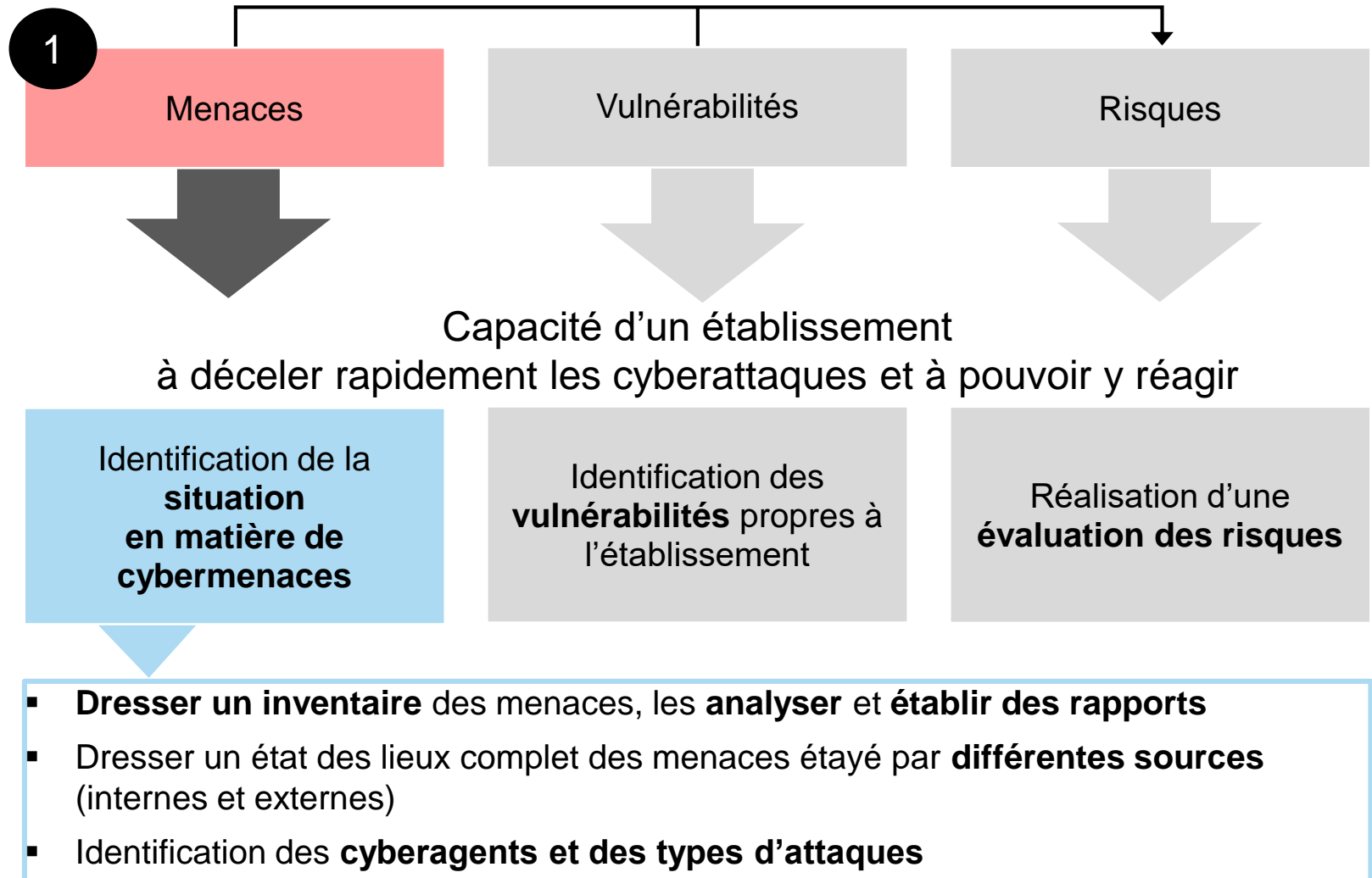
Les aspects essentiels



Identification des cyberattaques



Identification des cyberattaques







Inventaire des menaces – Qui sont les cyberagents ?

- **Groupes financés par des gouvernements**
- **Organisations criminelles**
- **Collaborateurs internes**
- **Pirates isolés**
- **Script kiddies**

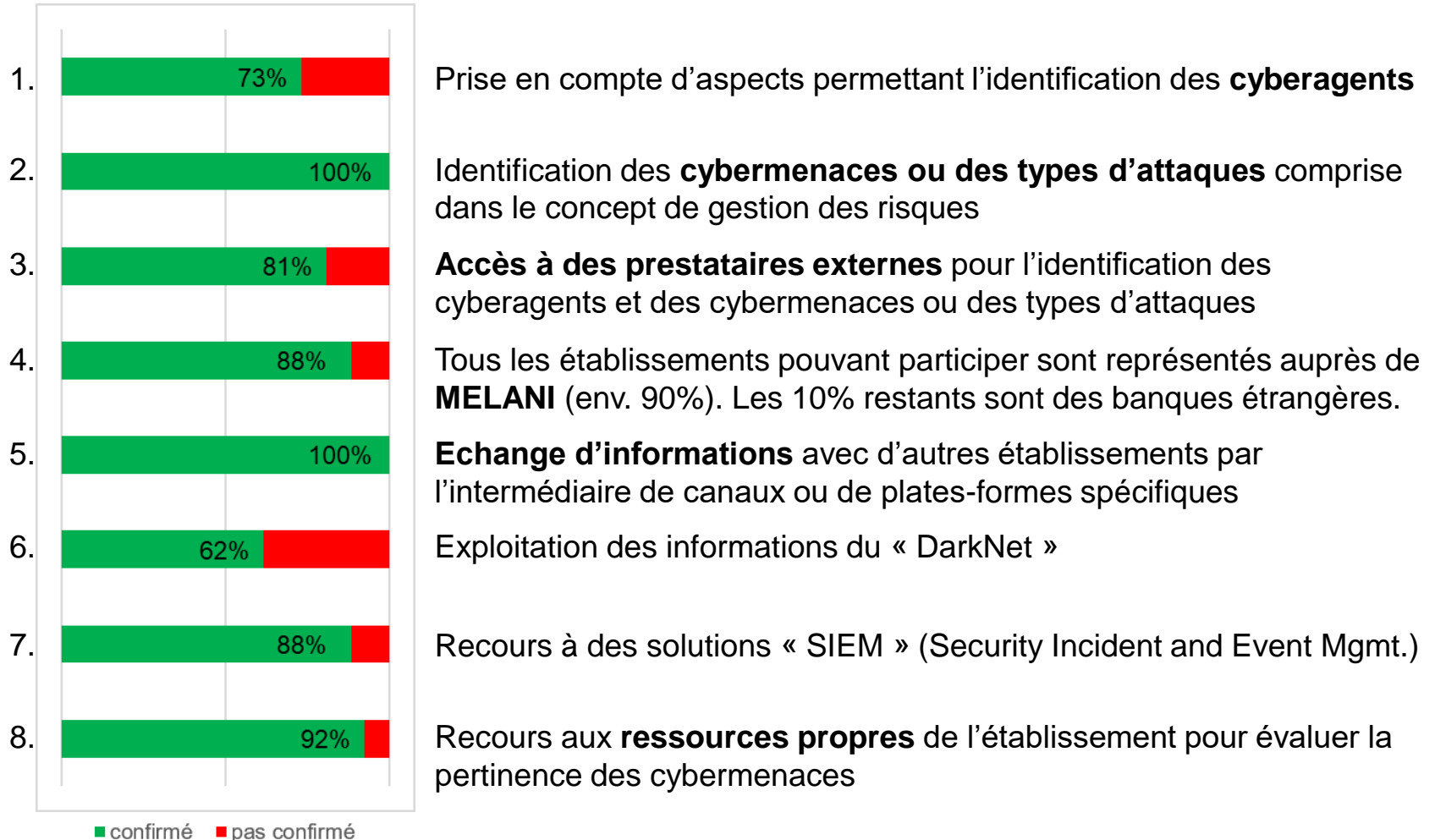


A quelles cybermenaces les banques en Suisse sont-elles exposées ?

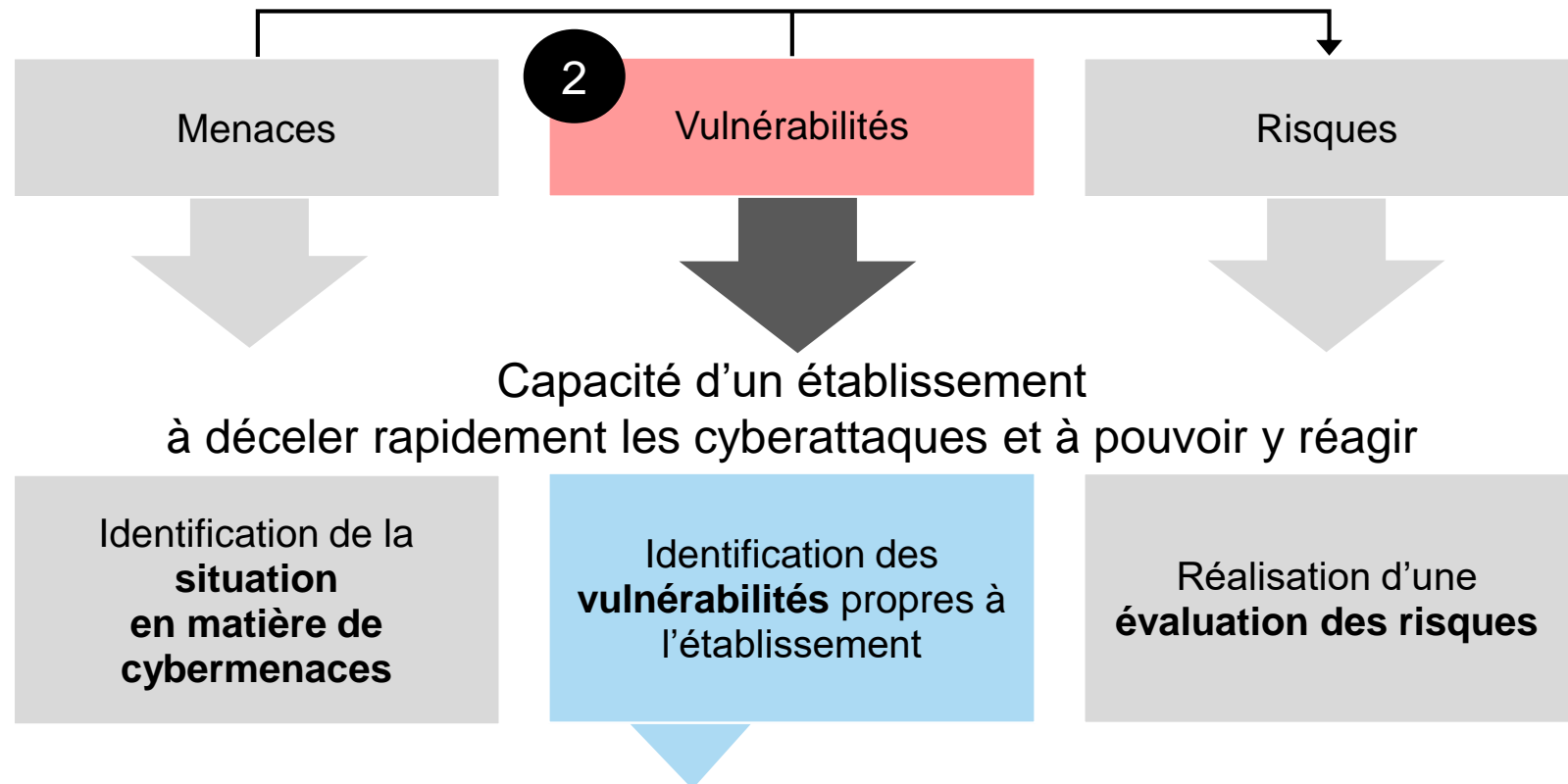
 <h3>4 APT</h3> <p>Advanced Persistent Threats (Generic) The term “advanced persistent threat” (APT) denotes a type of threat and attack that is technically sophisticated and usually present in...</p>	 <h3>1 CYBERCRIME</h3> <p>Cybercrime (Generic) The term “cybercrime” includes a wide range of criminal acts directed at individuals or enterprises. The specific background to calling a criminal act a “cybercrim... Phishing</p>	<h3>DDOS</h3> <p>Distributed Denial of Service (Generic) The term “denial of service” generally denotes an attack, or series of attacks, on an IT environment, with a view to disrupting or disabling the services p...</p>	<h3>INSIDER THREATS</h3> <p>Insider Threat (Generic) An insider threat is defined as the potential of an adverse act or omission from within the organization, i.e., committed by employees or individuals with a spec...</p>
 <h3>2 MALWARE</h3> <p>Malware (Generic) The term “malware” denotes any malicious software used for the purpose of attacking systems and IT environments. There is a vast number of malware specimens in th...</p>	<h3>MOBILE MALWARE</h3> <p>Mobile Malware (Generic) Mobile malware denotes a specific type of malware that affects mobile devices, most notably smartphones. The emergence of mobile malware has b...</p>	<h3>RANSOMWARE</h3> <p>Ransomware (Generic) The term “ransomware” denotes the insertion of malware that is designed to extort a ransom in money or money equivalent from the end user. This is usually ach...</p>	 <h3>3 SOCIAL ENGINEERING</h3> <p>Social Engineering (Generic) The term “social engineering” incorporates any and all human-intelligent interactions that are designed to elicit an involuntary or unconscious respons...</p>
<h3>UNPATCHED SYSTEMS</h3> <p>Unpatched Systems (Generic) Unpatched systems are programs for which a patch—software that modifies a system, application or other program—is either unavailable or ha...</p>	<h3>WATERING HOLE</h3> <p>Watering Hole (Generic) The term “watering hole” denotes a technique whereby end users visiting a certain web site are covertly redirected to another web site that will deliver ma...</p>		

Auto-évaluation 2018

1. Identification des menaces potentielles spécifiques à l'établissement

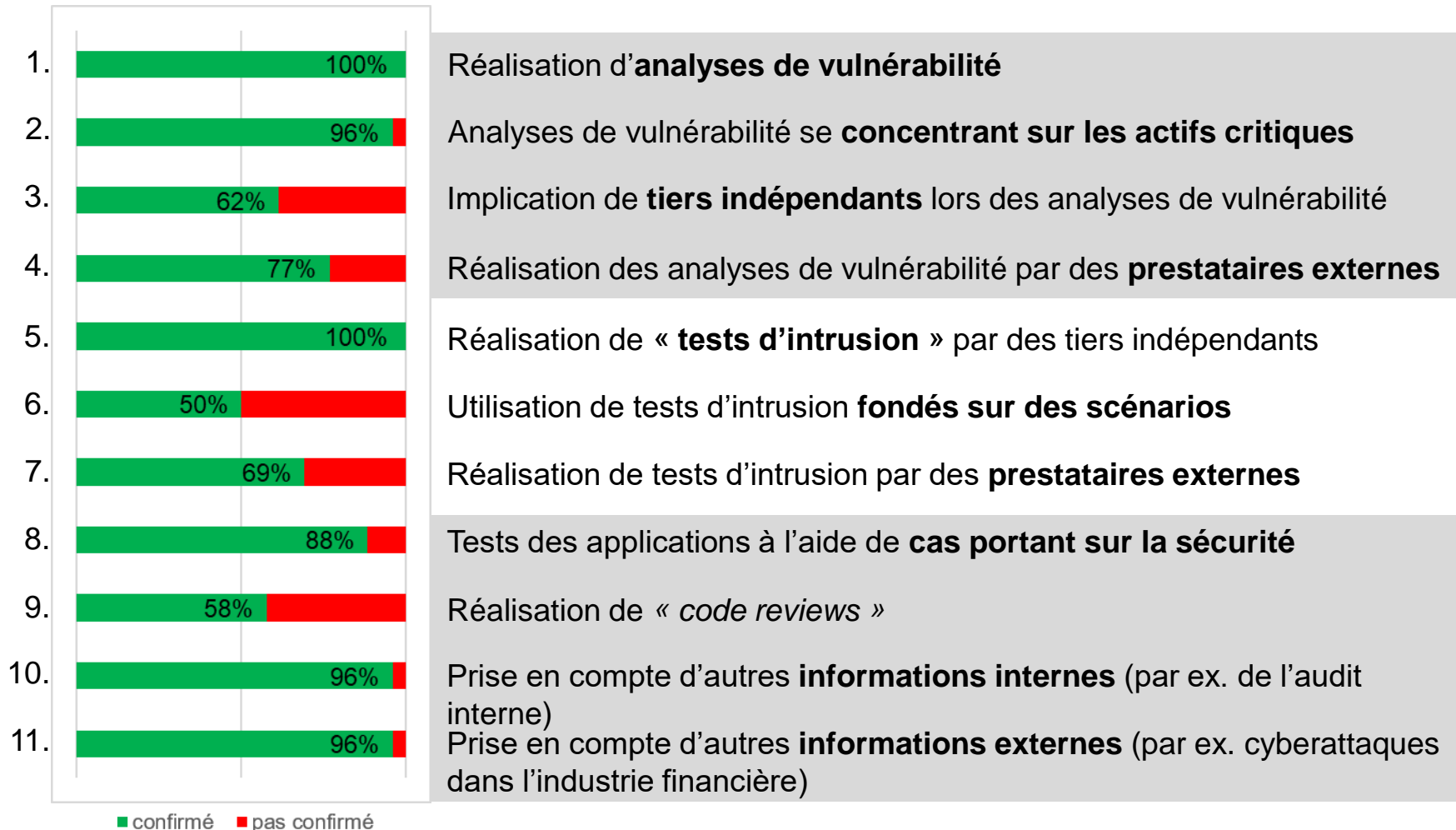


Identification des cyberattaques

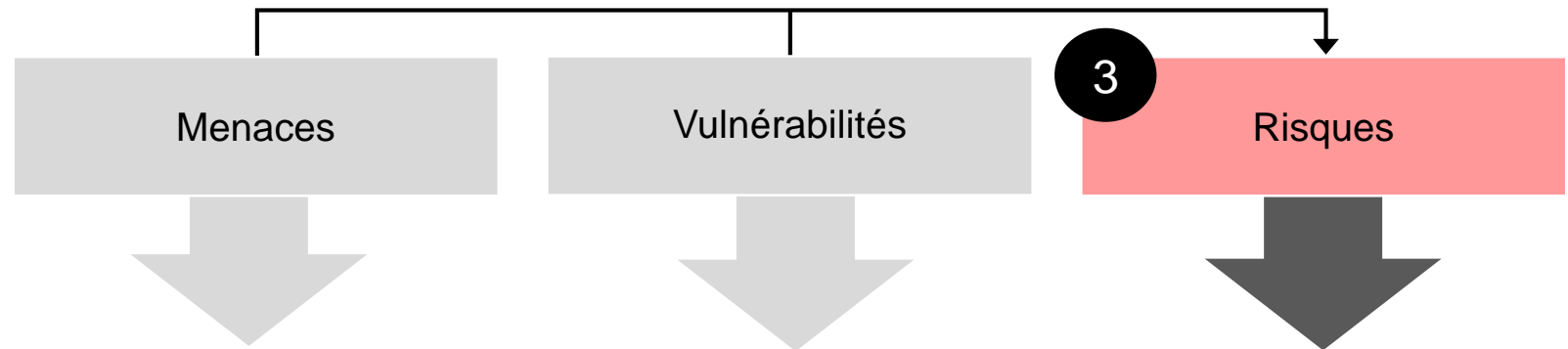


- **Détection** des points faibles, **classement** de ces derniers par ordre d'importance et établissement de **rapports** en conséquence
- Identification des **points faibles** dans le dispositif de protection des **actifs critiques**
- Recours à des **analyses de vulnérabilité** (par ex. « *scanning tools* », « *vendor notifications* ») et à des **tests d'intrusion**

2. Identification des vulnérabilités propres à l'établissement



Identification des cyberattaques



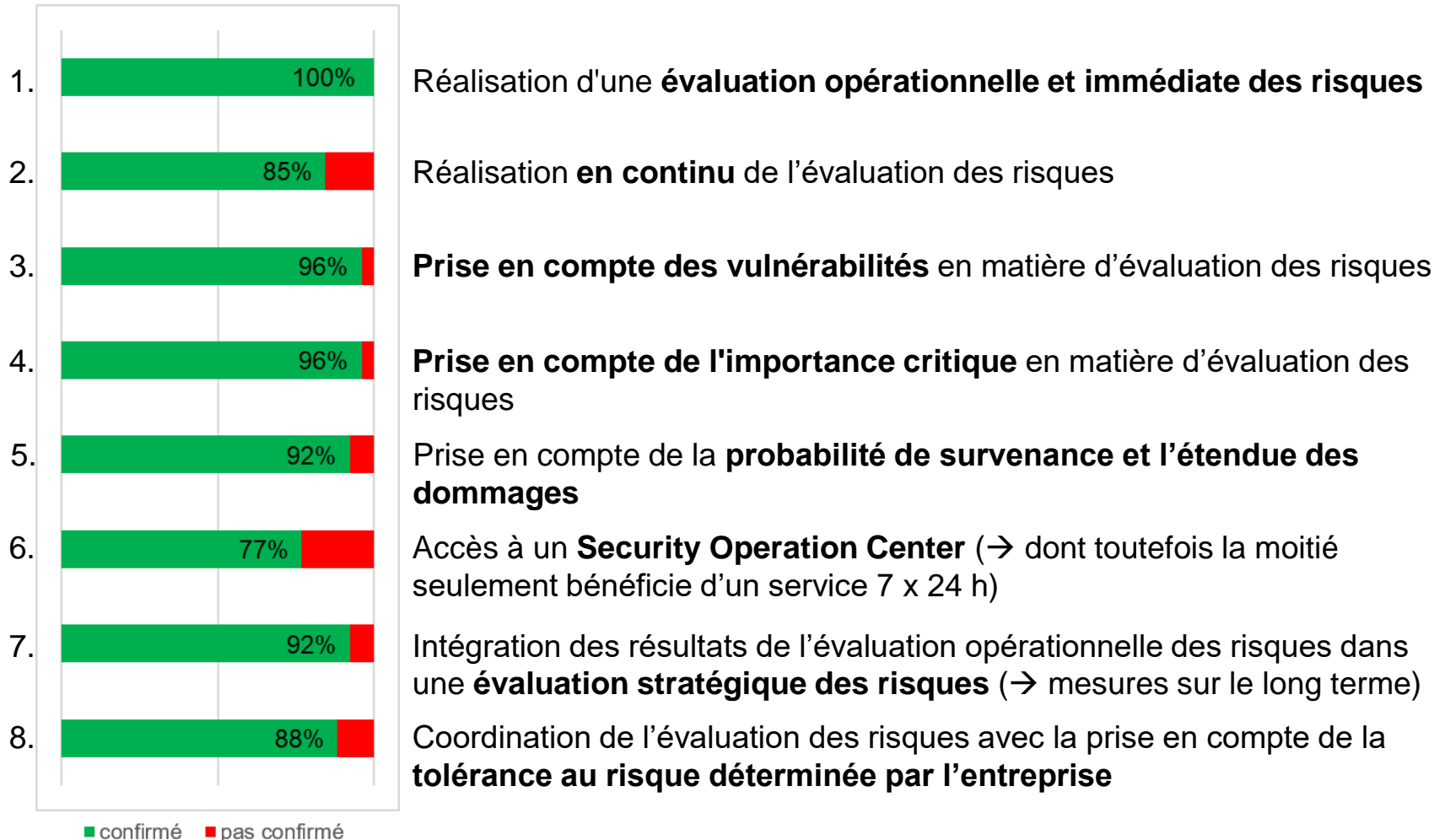
Capacité d'un établissement
à déceler rapidement les cyberattaques et à pouvoir y réagir



- **Corrélation** des **menaces** potentielles et des **vulnérabilités** spécifiques à l'établissement
- Evaluation de leur **gravité** au regard des **processus opérationnels et des composants critiques de l'infrastructure technologique**
- **Escalade** d'incidents touchant la sécurité informatique

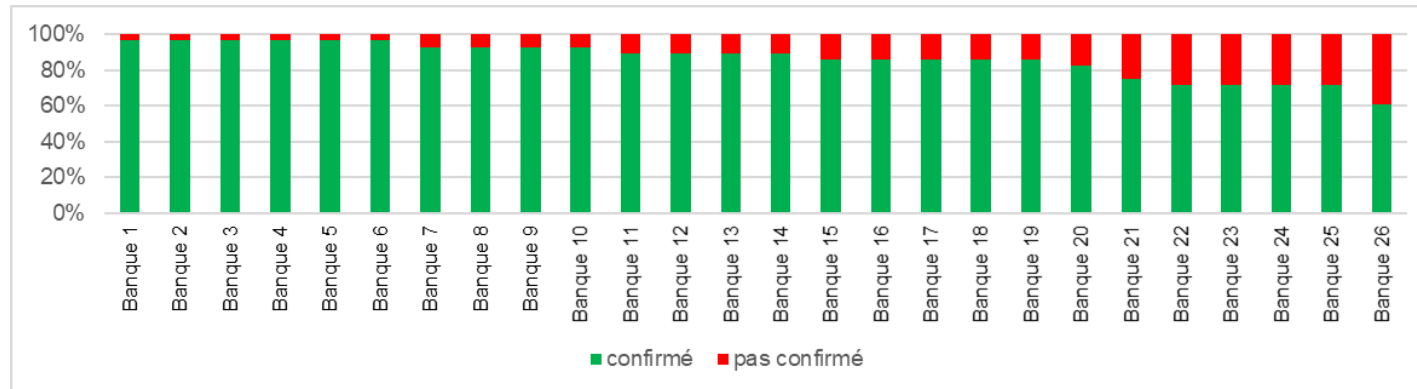
Auto-évaluation 2018

3. Réalisation d'une évaluation des risques



Auto-évaluation 2018

Comparaison des banques qui ont participé



Une confirmation de 100 % correspond à la prise en compte de la totalité des aspects essentiels au sens du questionnaire.

Conclusion de la FINMA

- Globalement, l'évaluation des réponses fournies par les **établissements participants** a montré que ces derniers ont **conscience** de cette thématique et que **la plupart d'entre eux ont pris des mesures**.
- Néanmoins, certains établissements **peuvent encore améliorer** la prise en compte des aspects essentiels au sens du questionnaire.
- L'évaluation a en particulier montré qu'en matière d'**identification des vulnérabilités**, les établissements participants n'ont pas encore tous atteint les principes de « *best practices* » dans l'ensemble des domaines.

CEO Fraud

Christophe Monigadon - CISSP

golem.de IT-NEWS FÜR PROFIS
 HOME TICKER VIDEO AUDIO FORUM
 TOP-THEMEN: 35C3 Raumfahrt 5G Security IT-Jobs Auto

CEO-FRAUD
Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge von Unternehmen. Mit fingierten E-Mails und Zahlungsanweisungen werden illegale Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen Automobilzulieferer getroffen.

Der deutsche Automobilzulieferer Leoni ist um rund 40 Millionen Euro betrogen worden, wie das Unternehmen am Dienstag selbst bekanntgegeben hat. Die Angreifer nutzten dabei offenbar eine als Chef-Trick oder CEO-Fraud bekannte Masche, um sich Zugriff auf die Zahlungen zu sichern.

Kantonspolizei Aargau
CEO-Betrüger treiben nun auch im Aargau ihr Unwesen

Mittwoch, 19.09.2018, 11:21 Uhr

- Die neue Masche heisst «CEO-Fraud». Man erhält vom (angeblich) eigenen Chef ein Mail mit der Anweisung, Bargeld ins Ausland zu überweisen.
- Die Kantonspolizei Aargau hat Kenntnis von mehreren derartigen Fällen. Adressaten der kriminellen Mails sind vor allem Vereine. Sie habe am Dienstag von mehreren Betrugsversuchen erfahren, teilt die Kantonspolizei Aargau mit. Unbekannte Absender von E-Mails hätten die Empfänger aufgefordert, für die Firma eine dringende Überweisung zu machen. Das Geld sei ins Ausland zu überweisen. Die Täter hätten sich als vorgesetzte Personen ausgegeben. Ob tatsächlich Geld überwiesen worden sei, weiss die Polizei noch nicht.

In einem Fall haben Büromitarbeiter den Kriminellen über 100'000 Franken überwiesen.

20 minuten de fr it
 Schweiz Ausland Wirtschaft Sport People Entertainment
 Zürich Bern Basel Zentralschweiz Ostschweiz

Gefälschtes Mail 16. August 2018 14:17; Akt: 16.08.2018 17:18

Sekretärin fällt auf CEO-Masche herein

Im Mai haben unbekannte Betrüger mit der Masche CEO-Betrug rund 80'000 Euro ergaunert. Die Kantonspolizei Thurgau mahnt zur Vorsicht.

Eine Sekretärin einer Thurgauer Firma hat Betrügern einen Betrag von 80'000 Euro überwiesen. (Bild: Keystone/Martin Ruetschi)

Abonnemente
 Menü Startseite Panorama Unglücksfälle und Verbrechen
Neue Zürcher Zeitung
Falsche Chefs täuschen Angestellte und erbeuten Millionen

Sie geben sich als Direktoren oder Firmen-Anwälte aus, imitieren deren E-Mail-Adressen und beauftragen dann Angestellte mit Transaktionen in Millionenhöhe auf ausländische Konten. Dieser «CEO-Betrug» hat Westschweizer Firmen 2015 Millionen gekostet.

27.1.2016, 14:02 Uhr
 (sda) Die Täter gehen dabei äusserst professionell vor, wie die Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik) auf ihrer Website schreibt: Angestellte werden zuerst telefonisch in einen fiktiven, dringlichen internationalen Unternehmenskauf im Ausland eingeweiht.

Sechs Millionen Franken Schaden in Genf

Am meisten betroffen von derartigen Betrugsfällen war im vergangenen Jahr der Kanton Genf. Dort gab es rund dreissig entsprechende Klagen mit einer Schadenssumme von sechs Millionen Franken, wie Marc Zingg von der Finanzabteilung bei der Genfer Kantonspolizei sagte. Er bestätigte damit eine Meldung der Zeitung «Le Matin Dimanche».

Weniger bekannt ist das Phänomen in der Deutschschweiz: Der Kanton Bern registrierte 2015 ein Dutzend CEO-Betrugsversuche für einen Gesamtbetrag von gegen zehn Millionen Franken, wie der Sprecher der Kantonspolizei, Nicolas Kessler, auf Anfrage sagte. In zehn Fällen waren die Täter erfolgreich und erbeuteten insgesamt rund 400'000 Franken.

Das Vorgehen kennt man auch im Kanton Genf, wo im vergangenen Jahr rund siebzig ähnliche Fälle bekannt wurden. Die Deliktsumme beläuft sich dabei auf rund 800'000 Franken. Gemäss Zingg werden den Genfer Behörden jede Woche ein bis zwei neue derartige Fälle gemeldet.

Nau.ch
 Home News Schweiz

Mails von falschem «Chef» im Umlauf

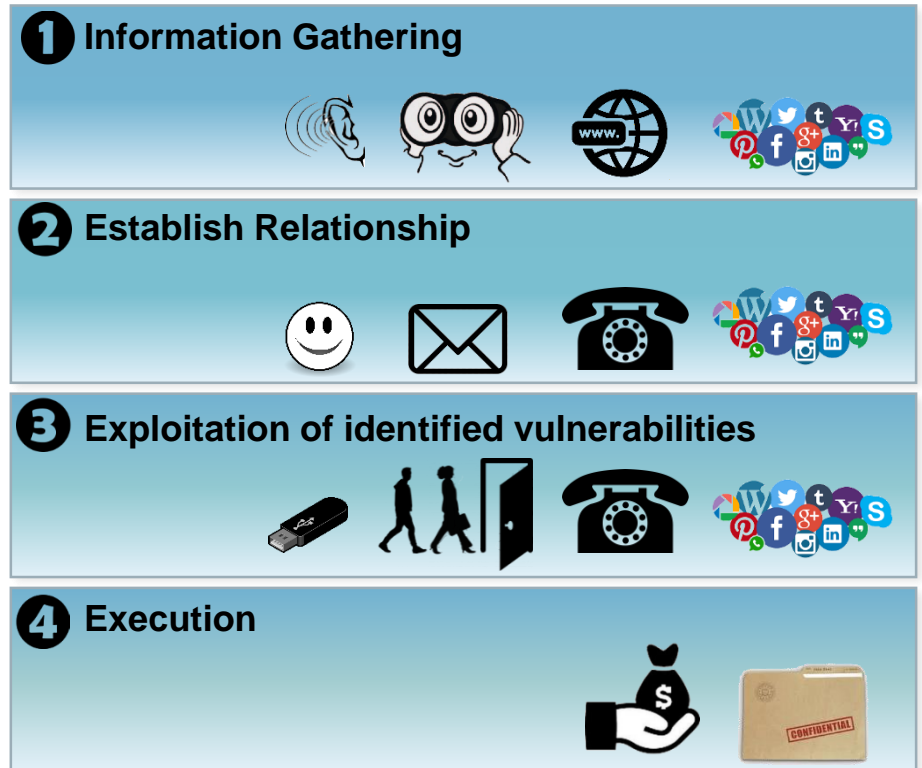
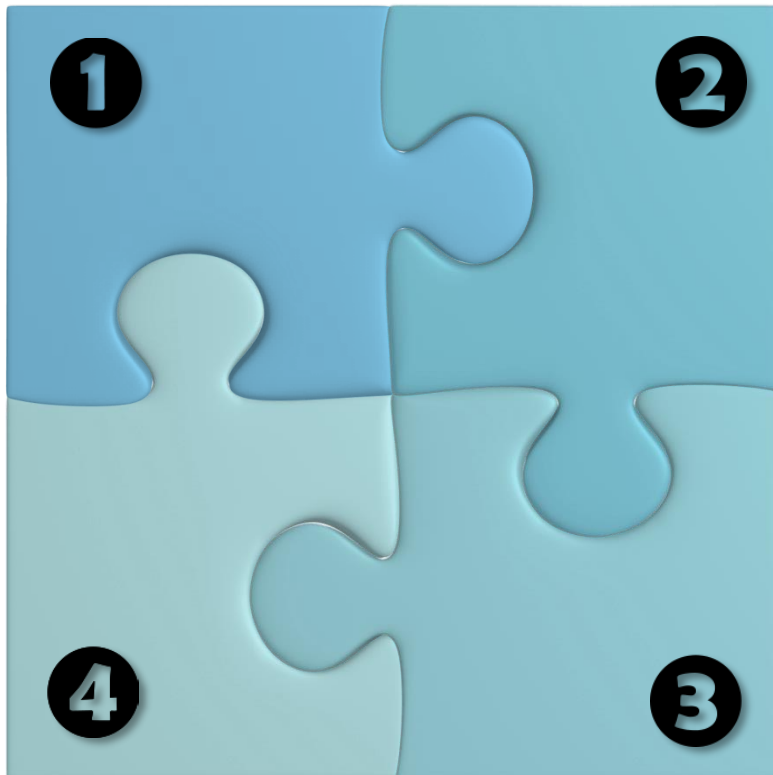
Luernerer Arbeitnehmer aufgepasst: In den vergangenen Wochen sind mehrere Fälle von so genanntem «CEO Fraud» bekannt geworden. Dabei werden Mitarbeiter mit gefälschten Mails gebeten, eine Zahlung auszulösen.

- <https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html>
- <https://www.srf.ch/news/regional/aargau-solothurn/kantonspolizei-aargau-ceo-betrueger-treiben-nun-auch-im-aargau-ih-unwesen>
- <https://www.20min.ch/schweiz/ostschweiz/story/Mit-CEO-Masche-betrogen-22194934>
- <https://www.nzz.ch/panorama/ungluecksfaelle-und-verbrechen/falsche-chefs-taueschen-angestellte-und-erbeuten-millionen-1.18684623>

Social Engineering

Definition: *The act of manipulation by one person to another to accomplish goals that may or may not be in the “target’s” best interest*

Social Engineering follows 4 steps:



CEO Fraud / CEO Impersonation

Definition: *CEO fraud involves impersonation of senior business managers, using social engineering to persuade employees to transfer their business money under the auspice of acceptable business intent and trust.*



KEY TARGETS:

Mid-level employees in financial or procurement services



HIGHLY ATTRACTIVE CRIME:

Large profits and low risk of detection



HIGH FINANCIAL IMPACT FOR TARGETED COMPANIES:

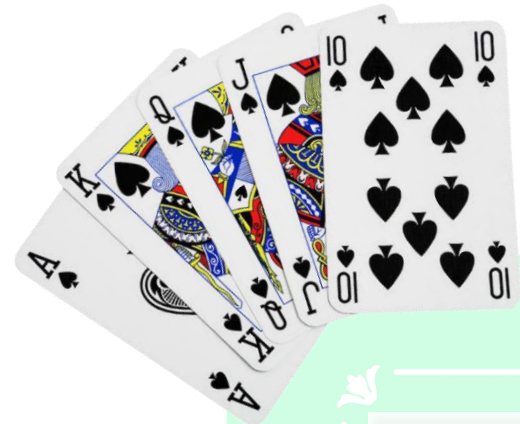
Losses up to several millions (€, \$, CHF, £ ...)



DIRECT HUMAN COSTS:

Shame, sanctions, loss of employment

PSYCHOLOGICAL TRICKS



GAIN THE TRUST OF THE TARGET:

Using stories with legitimate-seeming background



TIME PRESURE:

Create a situation where the “victim” does not have enough time to make a proper decision



HACKING:

Exploit weaknesses in email systems



PHISHING:

Send emails with stolen credentials



EMAIL SPOOFING – PHONE SPOOFING:

Disguising a communication from an unknown source as being from a known, trusted source



TYPOSQUATING:

use similar internet or e-mail addresses

How CEO Fraud works



Information Gathering

- OSINT, Website, Social Media, Phone, Dumpster diving,...



Establish Relationship

- A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)
- Requires an urgent transfer of funds and absolute confidentiality
- Invokes a sensitive situation (e.g. tax control; merger; acquisition)



Exploitation

- Pressures the employee not to follow the regular authorisation procedures
- Instructions on how to proceed are given later by a third-person or via e-mail



Execution

- The employee transfers funds to an account controlled by the fraudster.
- The money is re-transferred to accounts in multiple jurisdictions

Exemple tiré de la pratique : Le cas « lasertech »



Wilhelm Gross
Président du
conseil
d'administration



Bruno Meier
Directeur



Franz Müller
Directeur des
finances et de la
comptabilité



Alex Riley
Avocat
externe

Step 1 - Information Gathering



Information Gathering

- OSINT, Website, Social Media, Phone, Dumpster diving,...



Get the domain of your dreams!
Find and register a domain name and get free domain privacy for eligible domains.

example.com

xyz .com .online .site store

Site 77% off .XYZ domains. Get yours for just!

Sale prices 1st year only and do not apply to transfers or renewals. [View Full Pricing](#)

finma.report

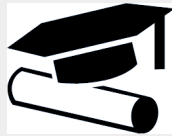
cliffordchance.partners

Step 2 - Establish Relationship

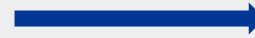


Establish Relationship

- A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)
- Requires an urgent transfer of funds and absolute confidentiality
- Invokes a sensitive situation (e.g. tax control; merger; acquisition)



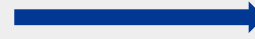
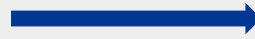
Alex Riley



Franz Müller



Wilhelm Gross



Franz Müller

Step 2 - Establish Relationship

Von: Wilhelm Gross <wilhelm.gross@lasertech.org>;
Gesendet: Dienstag, 26. November 2017 12:12
An: Müller Franz <franz.mueller@lasertech.org>
Cc: Dr. Alex Riley <alex.riley@cliffordchance.partners>
Betreff: FWD: RB GT9382



Wichtigkeit: Hoch

Guten Tag, Herr Müller

Hat Sie Dr. Riley bereits kontaktiert?

Ich würde Ihre Mitarbeit in einer Angelegenheit von Herrn Meier benötigen.

Wie flexibel sind Sie heute?

Mit freundlichen Grüßen
 Wilhelm Gross
 Präsident des Verwaltungsrats

Sent from my iPhone

Anfang der weitergeleiteten Nachricht:

Von: "Dr. Alex Riley" <alex.riley@cliffordchance.partners>

Betreff: RB GT9382

Datum: November 25, 2016 17:44:06 AM GMT+01:00

An: "Wilhelm Gross" <wilhelm.gross@lasertech.org>; <protokoll@finma.report>

Sehr geehrter Herr Gross,

Vielen Dank für die Benachrichtigung bezüglich Ihres Zeitfensters.

Um dieses einzuhalten, sollten wir folgende Punkte, vorrangig hinsichtlich der FINMA Richtlinien, die Sorgfältigkeitspflichten beachten:

Wie bereits erörtert, muss sämtliche Kommunikation im Rahmen der Buyer's Due Diligence und Data Room Vorgaben stattfinden.

d.h.:

- ausnahmslose Diskretion gegenüber allen Unbeteiligten dieser Übernahme (auch innerhalb der mitwirkenden Gesellschaften)
- interne digitale Kommunikation ausschliesslich schriftlich (E-Mail & Fax)
- protokollierter, lückenloser und chronologischer Kommunikationsverlauf (mich & die FINMA stets im CC der E-Mails verankern; respektive stets bei Antworten auf "Allen Antworten" klicken)
- vorherige Absprache beim Hinzuziehen weiterer Personen (mit Namens-, Status-, Kontaktangaben)

Dies sollte bis zur öffentlichen Bekanntmachung Ihrerseits durchgängig eingehalten werden.

Für die weiteren Schritte würden wir dringend einen Nachweis über die Transaktion benötigen, sodass wir das Vorkaufsrecht sichern können.

Optimal hierfür wäre die Transaktionsbestätigung **SWIFT MT103**.

Da ich weiterhin in Brüssel bin, können Sie mich in dringenden Notfällen weiterhin mobil erreichen.

Mit freundlichen Grüßen

DR. Alex RILEY

Rechtsanwalt
 Partner Mergers & Acquisitions
 Clifford Chance, Frankfurt

Step 3 - Exploitation

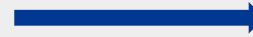


Exploitation

- Pressures the employee not to follow the regular authorisation procedures
- Instructions on how to proceed are given later by a third-person or via e-mail



Wilhelm Gross



Franz Müller

Step 3 - Exploitation

Von: Wilhelm Gross <wilhelm.gross@lasertech.org>; <protokoll@finma.report>

Gesendet: Dienstag, 26. November 2017 14:10

An: Müller Franz <franz.mueller@lasertech.org>

Cc: Dr. Alex Riley <alex.riley@cliffordchance.partners>

Betreff: Re: RB GT9382



Sehr geehrter Herr Müller

Wie sie vielleicht aus dem Anhang entnehmen konnten, bereiten wir mit Hilfe von Dr. Riley von Clifford Chance **eine Übernahme** vor.

Genau aus diesem Grund, waren Sie intern noch nicht informiert. Viele weitere aus unserem Hause sind es und sollten es auch bis zur öffentlichen Bekanntmachung auch nicht werden.

Beachten Sie bitte, dass einige Richtlinien der FINMA eingehalten werden müssen.

Erwartet wird **absolute Diskretion** (auch innert der Gesellschaft) und lückenloser Nachweis über unsere Kommunikation (stets "Allen Antworten", sodass auch Dr. Riley und das Protokoll beachtet werden).

Um ein Vorkaufsrecht zu sichern, müssen wir eine Zahlung ins Ausland i.d.H. von EURO

1'172'000.00 tätigen.

Welches wäre der einfachste und effektivste Weg, dies **am heutigen Tage** abzuwickeln, sodass wir eine Zahlungsbestätigung einreichen können?

Mit freundlichen Grüßen

Wilhelm Gross
Präsident des Verwaltungsrats

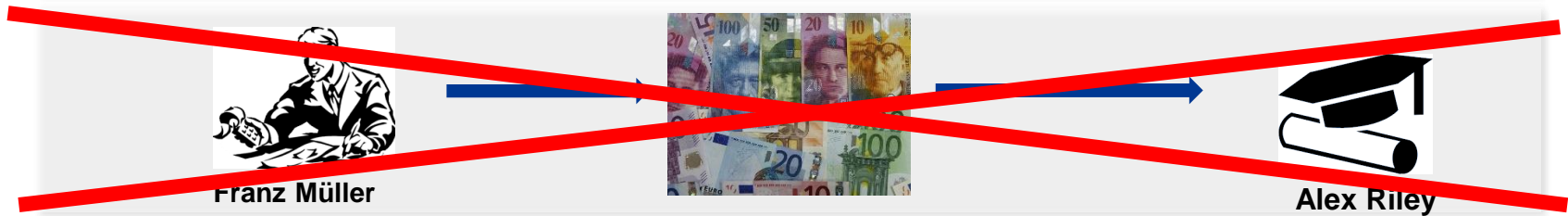
Sent from my iPhone

Step 4 - Execution



Execution

- The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions



Lessons learned

at the company level:

- Be aware of the risks and spread the information within the company.
- Avoid sharing sensitive information on the company's hierarchy, security or procedures.
- Have robust funds transfer processes
- Finding out who owns a Internet domain similar to yours
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.
-

as an employee:

- Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- Always carefully check e-mail addresses when dealing with sensitive information/money transfers.
- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
-