Cybersecurity

Is Cyber risk just another behavioural risk?

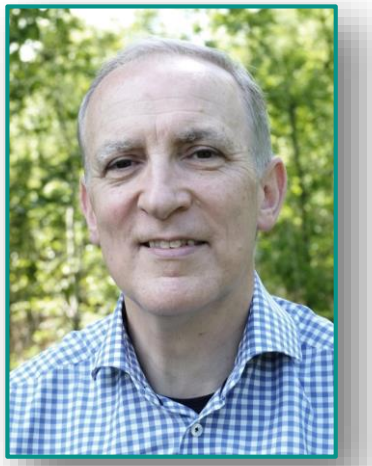
What is the role of the human factor and how can internal audit challenge the existing practices?

International round table organised by the European Internal Auditors and the European Confederation of Internal Auditing (ECIIA)

Round table panellists

Pascale Vandenbussche
ECIIA Secretary General
Facilitator

Guy-Philippe Goldstein
Advisor to PwC France
Autor of the expert's note in the Cyber Practical Guidance



Twan Oosterveld
Group Internal Audit - IT audit & security
Citco

Luca Laguardia
Head of Internal Audit
Borsa Italiana – AIIA Cybersecurity Observatory

Marc Solé
Operational & IT Risk Audit Director
Banco Sabadell

Context

42 CAEs and Audit Committee Chairs interviewed

579 survey respondents +10% annual increase

51 experts interviewed

Download the documents here

Why is human factor important in cybersecurity ?

Cyber risks : Corporations #1 risk !

Evolution of corporate cyber-risk appraisal

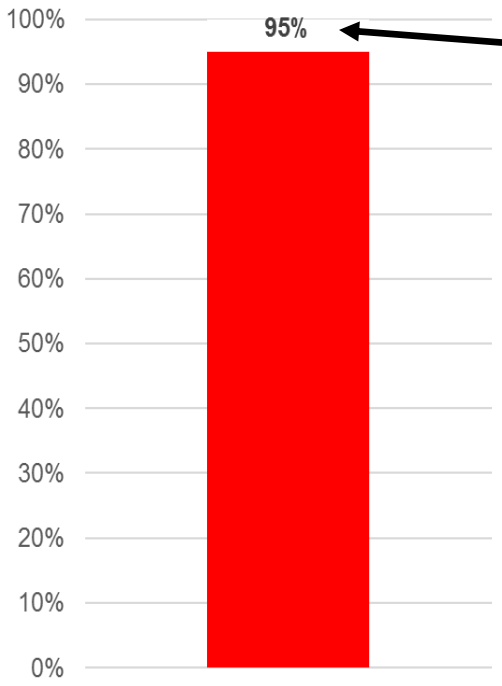
ECIIA / Risk In Focus 2017-2021

Risk in Focus 2017-2020	Risk in Focus 2021	Risk in Focus 2022+ ?
Top 3 Corporate Risk	**#1 Corporate Risk**	

The human factor

At the employee level

% of cyber incidents with "human error" as contributing factor[1]



Includes:

- **"Double clicking" on an infected attachment or unsafe URL**
- Use of default user names & passwords
- **Easy-to-guess passwords**
- Lost laptops or mobile devices
- **Disclosure of regulated information via use of an incorrect email error**
- System misconfiguration
- Poor patch management

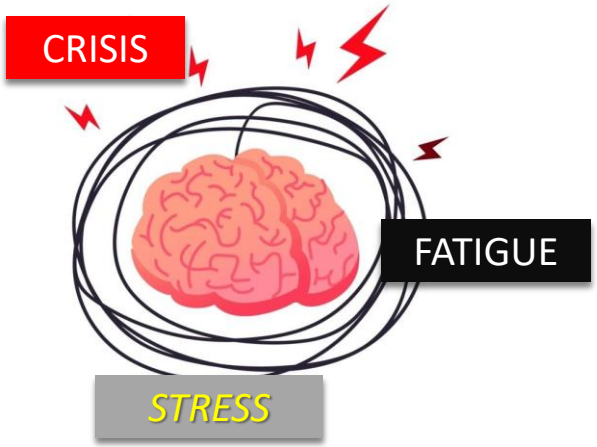
- **52% of ICS cybersecurity incidents[2]**
- **In 52% of cases, the human factor is the most important factor [3]**

Source:
1/IBM Security Services 2014 Cyber Security Intelligence Index; 2/ Kaspersky 2019; 3/ CompTia 2015 – "human error accounts for 52 percent of root causes of security breaches, while technology errors account for 48 percent", in CSO Online @ https://www.csoonline.com/article/2908475/surveys-employees-at-fault-in-majority-of-breaches.html

The human factor

Why? What happens at the employee level?

Cognitive limitations



No respect for established protocols

- **61% of respondants admit to mismanage documents (not suppressed/ not stored at the right place/send to the wrong sender)**
- **44% to 66% do not respect security protocols all the time**
- **20%-25% may upload unauthorized media/ log on unauthorized sites and suppress security controls to do so**

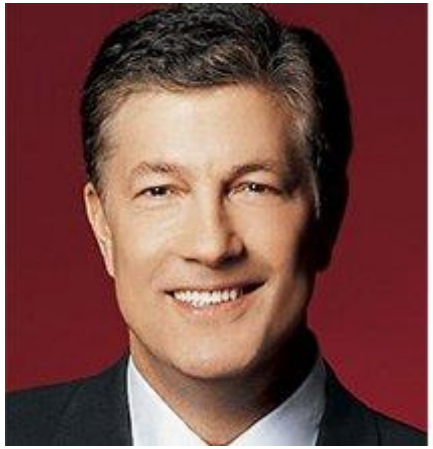
Source: Big Brotther Watch 2016, CybSafe/ UK Information Commissioner's Office 2019, Kaspersky 2017

Insider threat (rare)

The human factor

The corporate organisation - Leadership

Beth Jacob
Target CIO



Gregg Steinhafel
Target Chairman
President & CEO

Chris Coonan
Landmark White CEO

Chris Hylen
Imperva CEO

The human factor

The Corporate organisation – Preparedness & Culture

State of Preparedness

(Survey of 343 French IT & Security Executives – IBM Ponamon, 2020)

- **80% of companies: no robust incident response plans**
  - **24% partial only**
  - **31% informal**
  - **25% do not have any**
- **Issues with the 20% remaining:**
  - **48% have not tested the plan for at least a year**

Importance of Culture

Eugene E. Habiger,

- *Commander in Chief, Strat Command (nucléaire militaire)*

"Good security is 20% equipment and 80% people »

- **Overall stress level?**
- **Protocols complexity?**
- **Punitive culture?**
- **…Investment in training?**

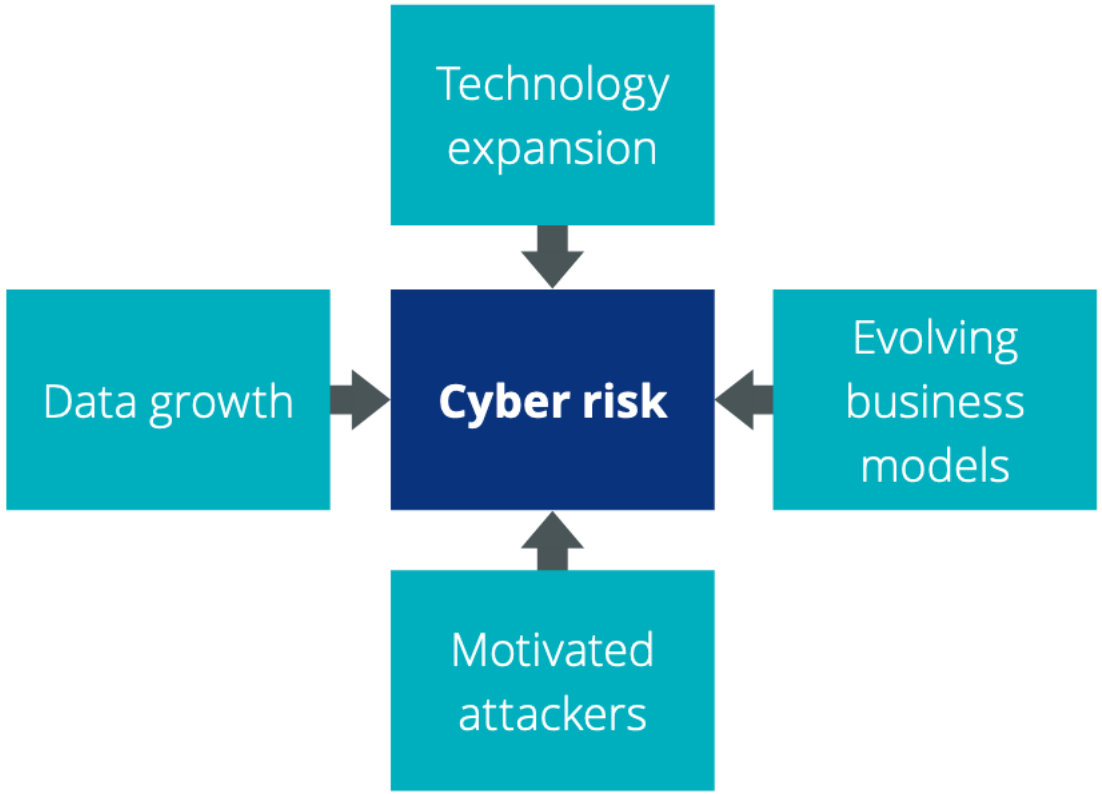
PANEL DISCUSSION

Over the years, cyber risks has remained a priority for businesses, but companies still face major cyber attacks.

How can we explain such difficulties to meet the challenge?

Twan Oosterveld

Cyber risks and -security



Guy-Philippe mentioned the importance of security culture in cyber risk management.

Is that particular aspect covered by your audit plans?

Luca Laguardia

The publication highlighted the need for companies to « prepare for the worst ».

What is the contribution of internal auditing in your respective compagnies?

What about specific focus on human factor?

Marc Solé and Twan Oosterveld

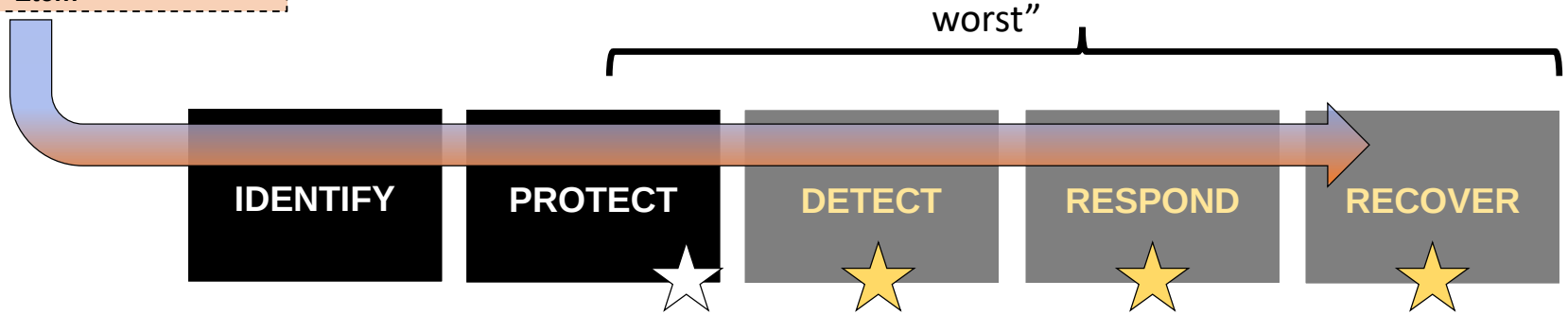
Assess processes and controls assuming that human errors and mistakes will happen…

ATTACKS / RISK FROM WITHIN

(Human Factor)

Virus / malware / ransomware
Social engineering (Phishing,..)
CEO Fraud
Careless / uninformed employees
Loss of devices
Etc…

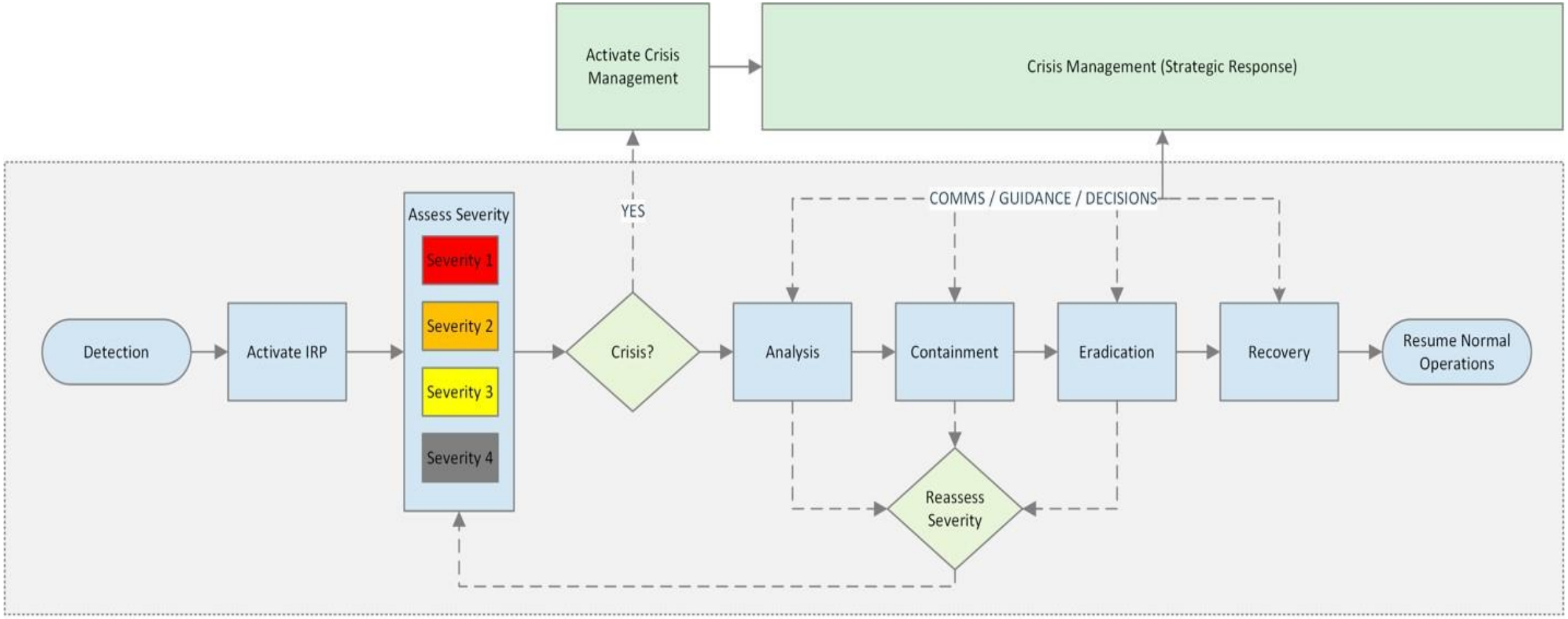
- "Prepare for the worst"



- Do not forget audit focus

Incident Vs Crisis

How crisis management integrates incident management



Auditing Cyber exercises

Technology

Operational

Business

Impact Assessment

- **Customers**
- **Employees**
- **3rd parties,..**

- **Operations**
- **Key Business processes**

Cybersecurity response

Coordination with law enforcement agencies

Legal / Regulatory

Notifications to Regulators

Communication Management

Communication with key stakeholders

- Customers
- Employees
- Media
- Others

The weakest link

Preparing the practical guidance, we identified very few publication to help internal auditors to build their competences regarding auditing the impact of human factor in cyber risk management.

If you wish to share a key good practice, what would it be?

Luca Laguardia and Marc Solé

OPEN QUESTIONS

THANKS!

- To access the Practical Guidance
- To watch the replay
- To access to the key findings

Visit the ECIIA Website !