

# Risk approach

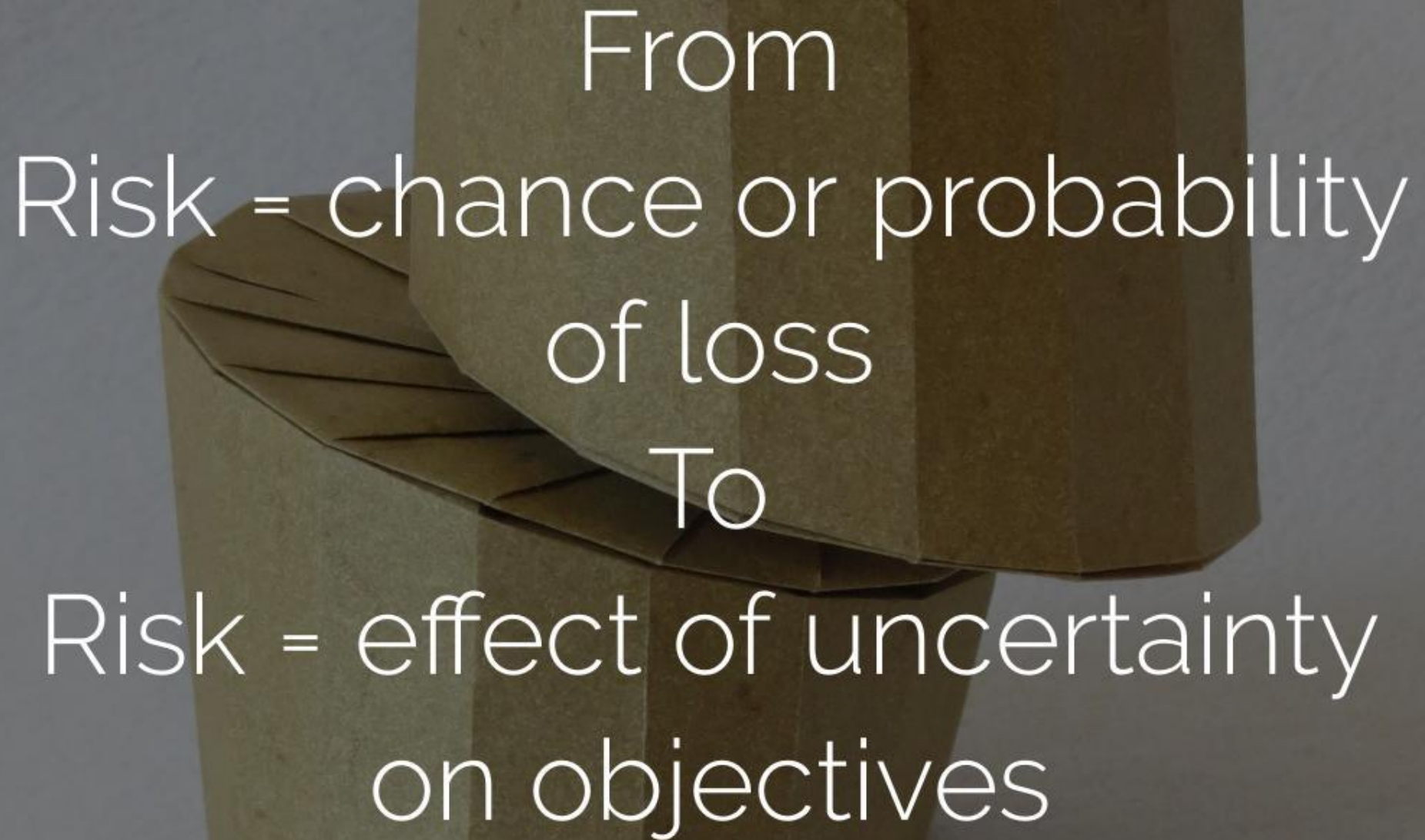


goes spare

A photograph of a stack of books, viewed from a low angle, showing the edges of the pages and the spines. The books are stacked in a slightly irregular manner, with some pages visible. A dark, semi-transparent horizontal band is overlaid across the middle of the image, containing the text 'ISO 31000' in large white letters and 'a paradigm shift' in smaller white letters below it.

# ISO 31000

a paradigm shift

The background of the slide features two brown paper bags, likely for coffee or tea, stacked one on top of the other. The bags are made of a textured, fibrous material and have a simple, cylindrical shape with a folded top. The lighting is soft, highlighting the texture of the paper. Overlaid on this image is white text that defines the concept of risk in two different ways.

From  
Risk = chance or probability  
of loss  
To  
Risk = effect of uncertainty  
on objectives



# How to deal with risk

1. Avoiding the risk by deciding not to start or continue with the activity
2. Accepting or increasing the risk in order to pursue an opportunity
3. Removing the risk source
4. Changing the likelihood
5. Changing the consequences
6. Sharing the risk with another party
7. Retaining the risk by informed decision

# Cybersecurity Risk theory

ISO/IEC 27005



# XSS

privilege  
escalation

# Vulnerability

Technical or HUMAN

# SQL injection

# Threat

Opportunistic, Targeted or Organized







# impact

Tangible or Intangible



A photograph of a brick wall covered in graffiti. The graffiti includes large yellow letters with black outlines, red spray-painted marks, and a tag that reads "R.I.P. MCA.". A semi-transparent black banner is overlaid across the center of the image, containing the text "RISK = VULNERABILTY \* THREAT \* IMPACT" in white, bold, sans-serif capital letters.

**RISK = VULNERABILTY \* THREAT \* IMPACT**





There is no such thing as zero-risk, always consider the:

# Residual RISK

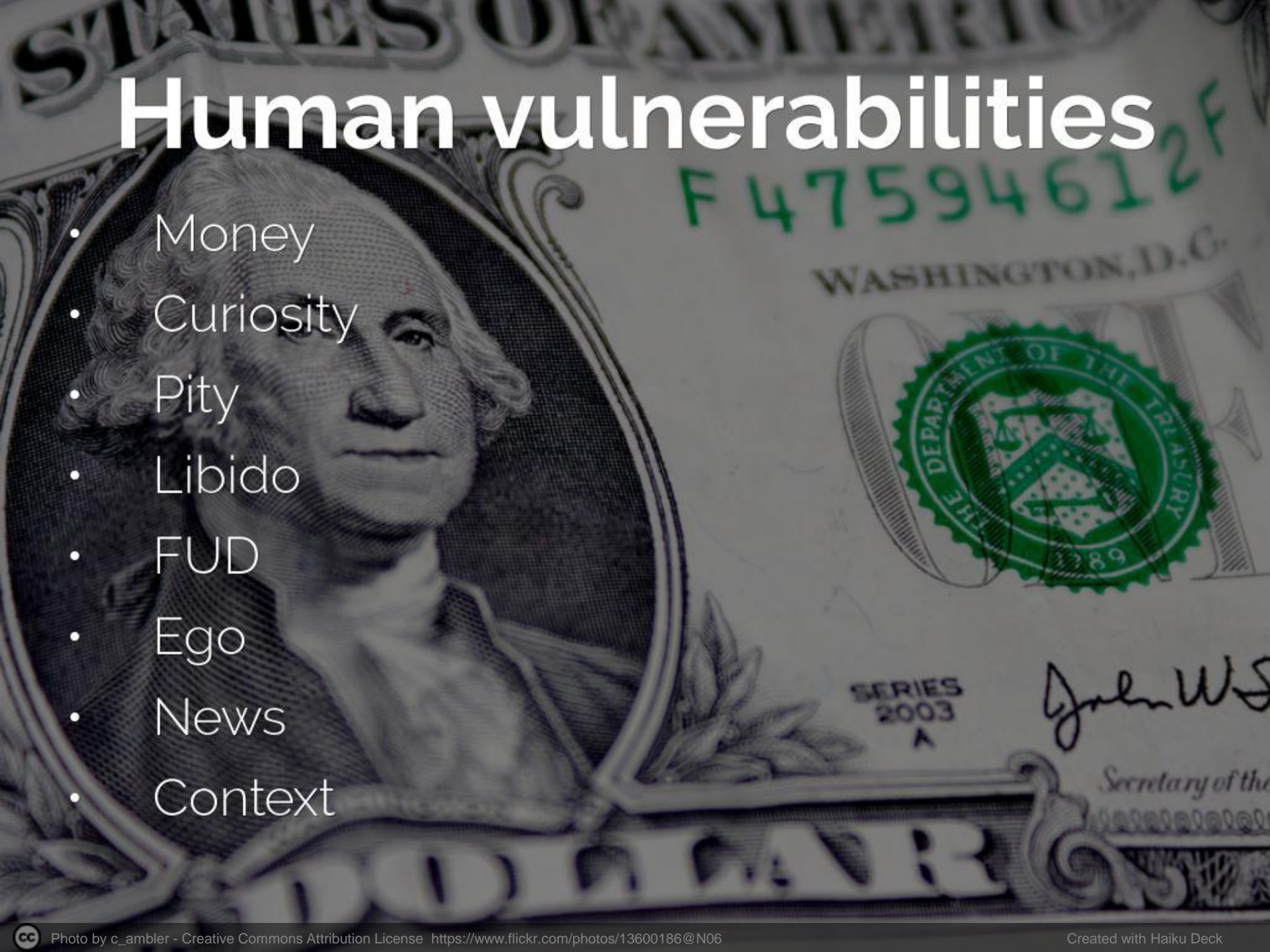




# Know your vulnerabilities

# Human vulnerabilities

- Money
- Curiosity
- Pity
- Libido
- FUD
- Ego
- News
- Context



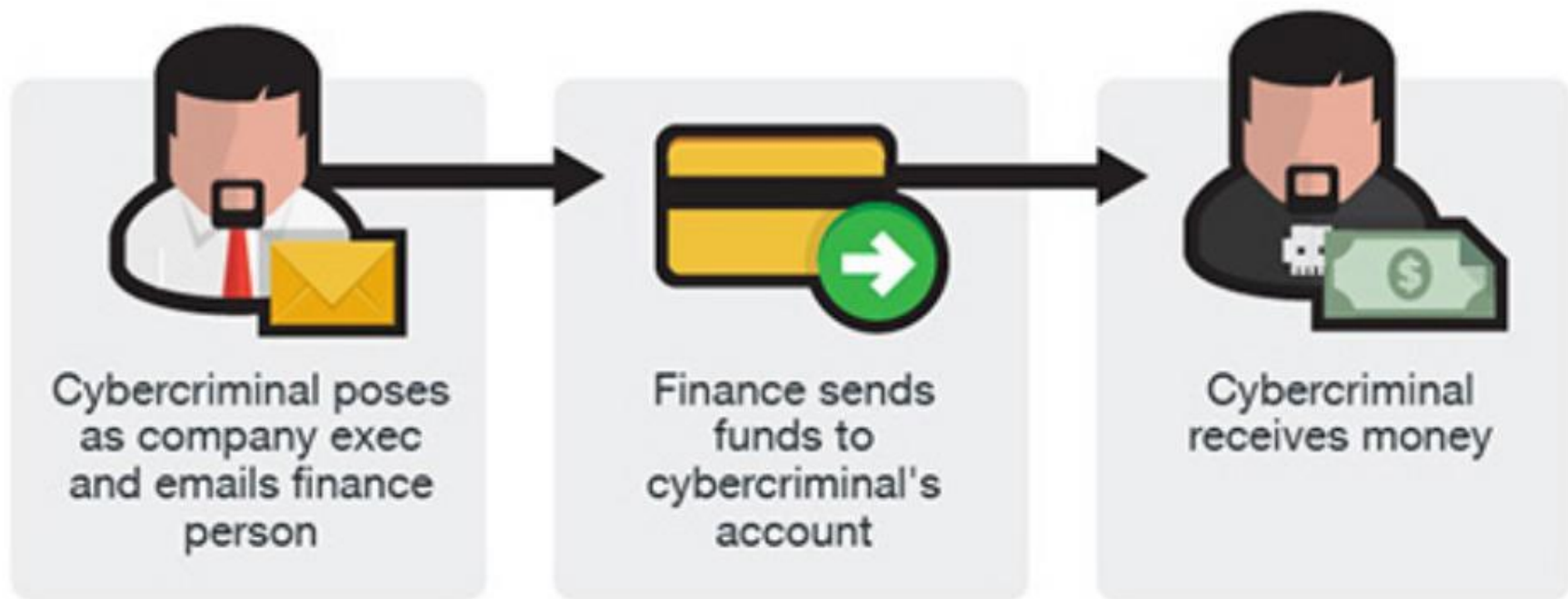


# Alfred W. - CEO, Octopus Group



Victim of "CEO FRAUD", his reputation is at stake

# CEO fraud (a BEC scheme)





# Invoice scam scheme



Cybercriminal compromises employee email



Compromised account is used to send notifications to customers



Payments are transferred to cybercriminal's account



Cybercriminal receives money

# BEC schemes (2013-2015) by Trendmicro

22K

---

victims

79

---

countries

3G\$

---

estimated loss



# 2016, year of the ransomware

## Ransomware 2016 in numbers

**62**

new ransomware families appeared



The number of new ransomware modifications increased

**11 - FOLD**

2,900  
Q1

32,091

Q3



**An individual attacked**

Q1

every  
20 seconds

Q3

every  
10 seconds

**A business attacked**

Q1

every  
2 minutes

Q3

every  
40 seconds

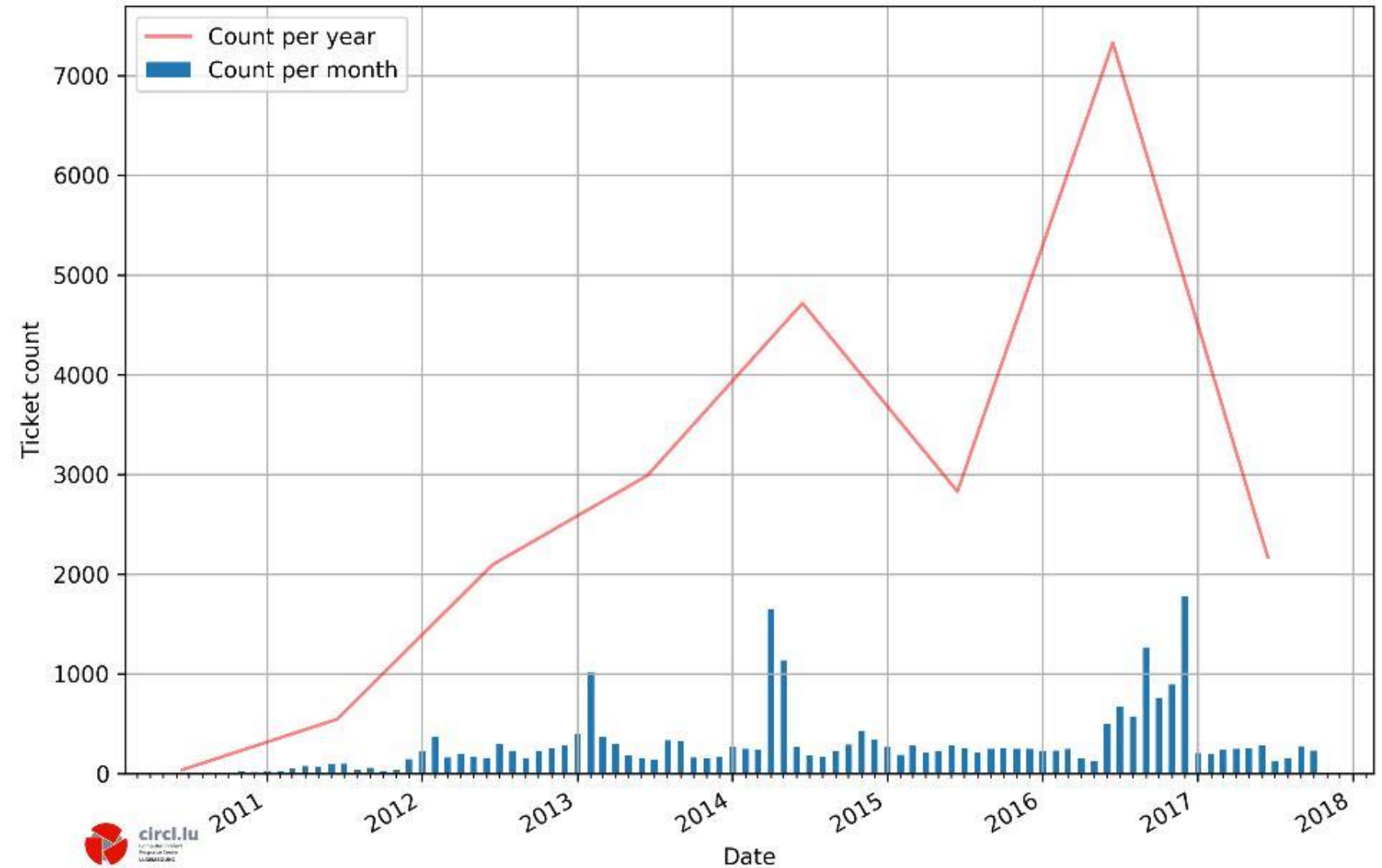


**One in five**

SMBs who paid the ransom  
**never got their  
data back**

All the statistics were obtained using Kaspersky Security Network (KSN)  
© 2016 AO Kaspersky Lab. All Rights Reserved.

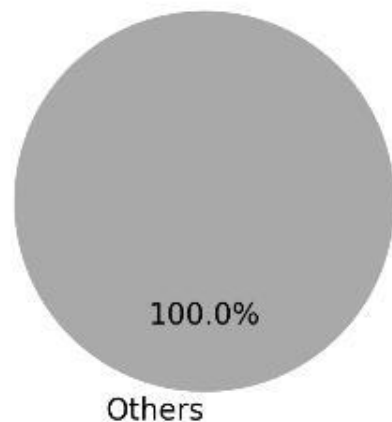
# Number of ticket overtime



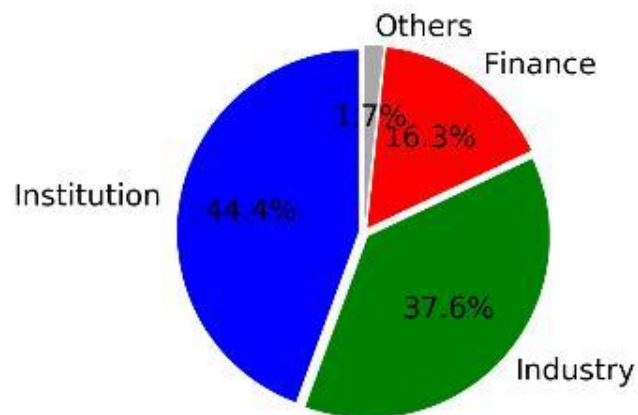


# Ticket category repartition

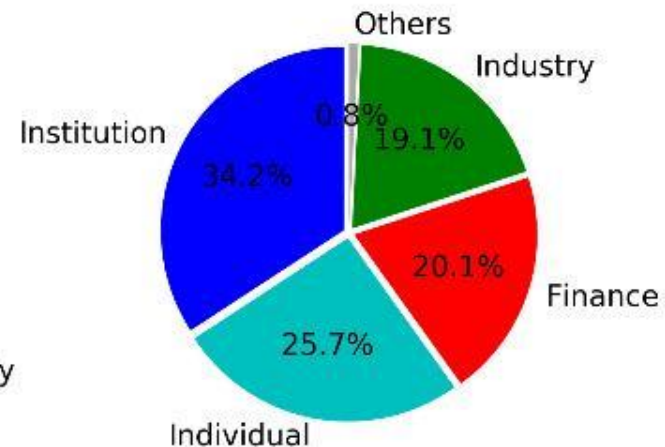
2011



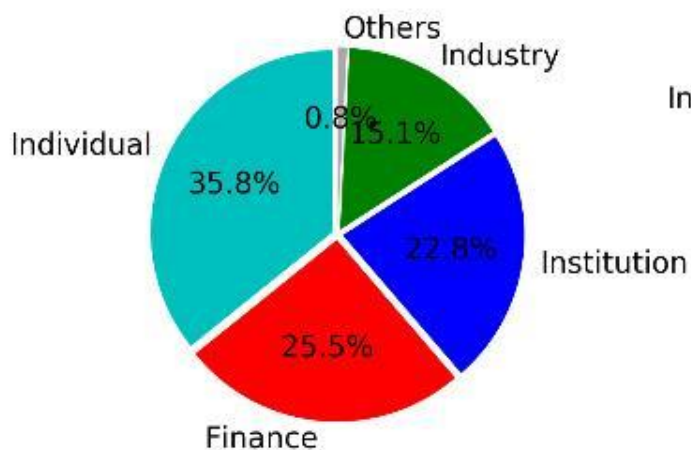
2012



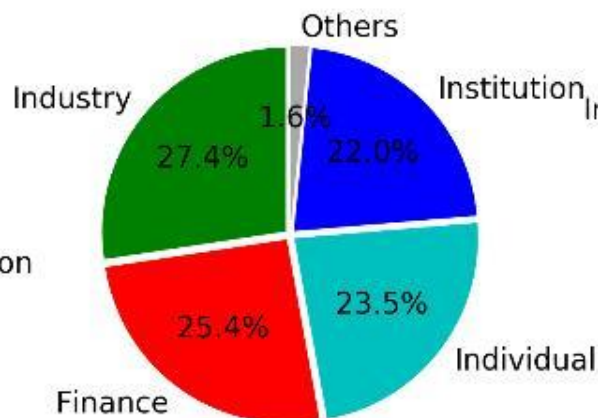
2013



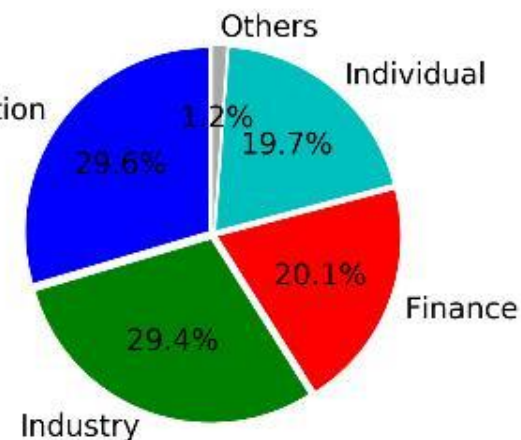
2014



2015



2016





# Defence in Depth

Prevent, Detect, React, Recover



# Prevention...

- PEOPLE (awareness ,training, competences...)
- TECHNOLOGY (AV, WAF, IPS, SIEM, SUS...)
- ORGANIZATION (policies, procedures, responsibilities...)
- COMPLIANCE (privacy, IP, notification...)

**CAUTION**

**THIS MACHINE  
HAS NO BRAIN  
USE YOUR OWN**





# ...is not enough !

- manage risks (CISO)
- be proactive, detect & react (CERT)
- be ready, prepare for a crisis
- have a BCP/DRP
- get an insurance

**DON'T WAIT  
TO BE HUNTED.  
PROTECT  
YOUR DATA.**

**[www.securitymadein.lu](http://www.securitymadein.lu)**

**nor suffer in silence**





# Demo Time

MONARC - Optimised Risk Analysis Method



# Thank you for your attention

Pascal Steichen - CEO SECURITYMADEIN.LU