



# From Hacker to CISO

How to turn risk management into a business differentiator

Feb 2020 ISF General Assembly





# Who am I?



**CISO  
Business Enabler  
Tech and Auto-  
Enthusiast**

**Hobby-Photographer  
Hobby-Chef**



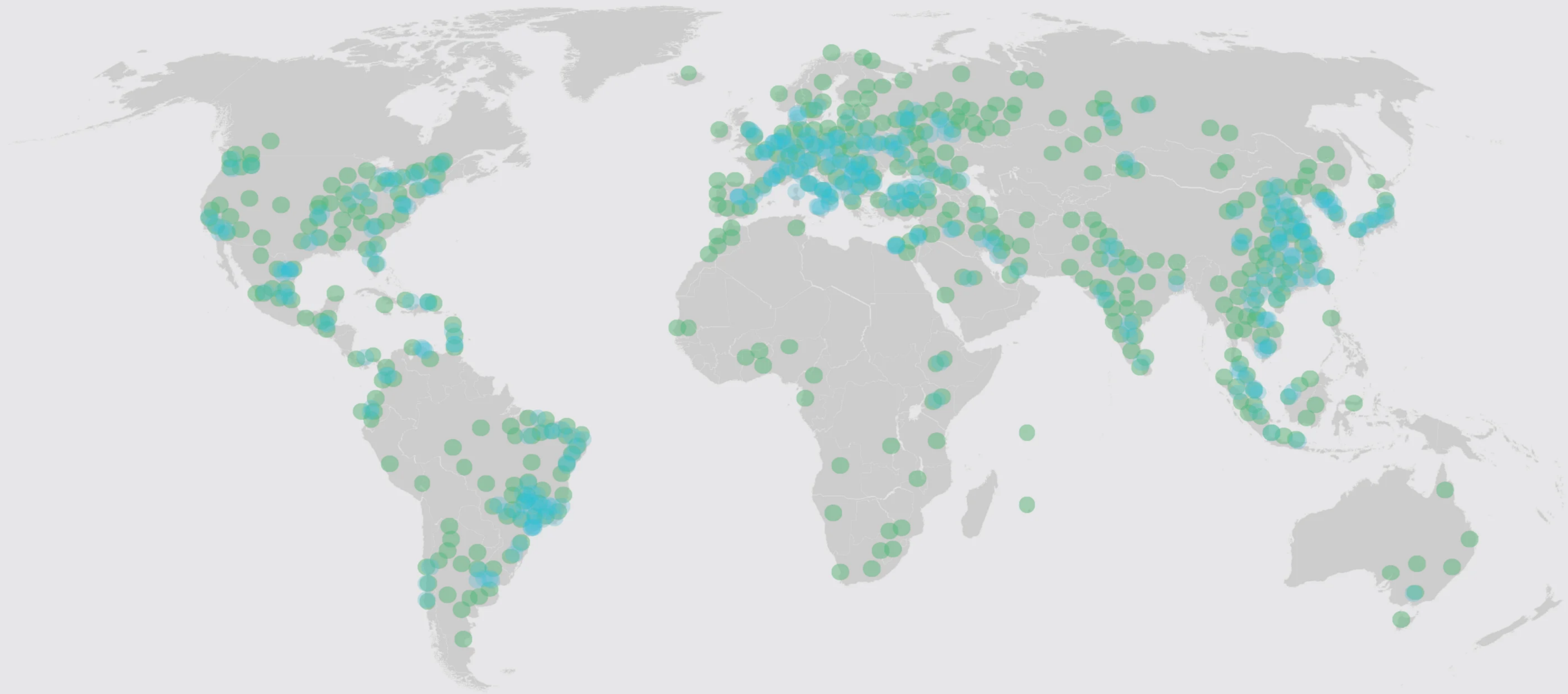


# Cyber Threat Landscape Finance Sector





## EXHIBIT 1 | Cyberattacks Are Proliferating Worldwide



**Source:** QuoScient.

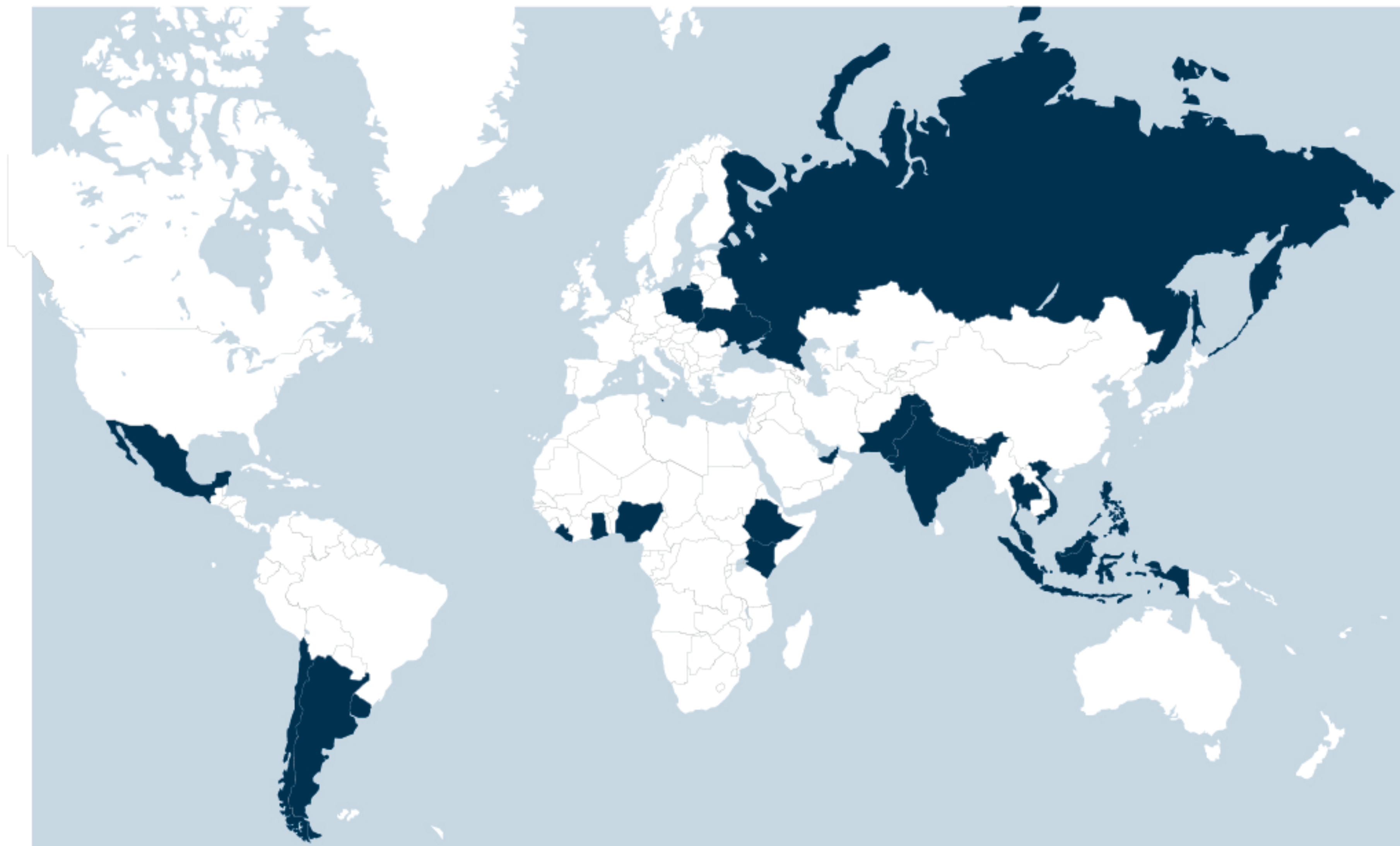
**Note:** The colored circles show the origin of all cyberattacks detected by QuoScient sensors on June 13, 2018, ranging from the smallest number (light green) to the largest number (dark blue).





FIGURE 1

## Geolocations of Payment System Attacks, 2016-2018







# The Geography of financial attacks by Lazarus group

The malware by Lazarus group, infamous for its theft of \$81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.







# Cobalt Group

## Key facts

Banks of at least 14 countries including Russia, the UK, the Netherlands and Malaysia have suffered the attacks from this criminal group.

The 'touchless jackpotting' technique employed does not involve any physical manipulations of ATMs.

Bank systems are infected using tools that are widely available in public sources.

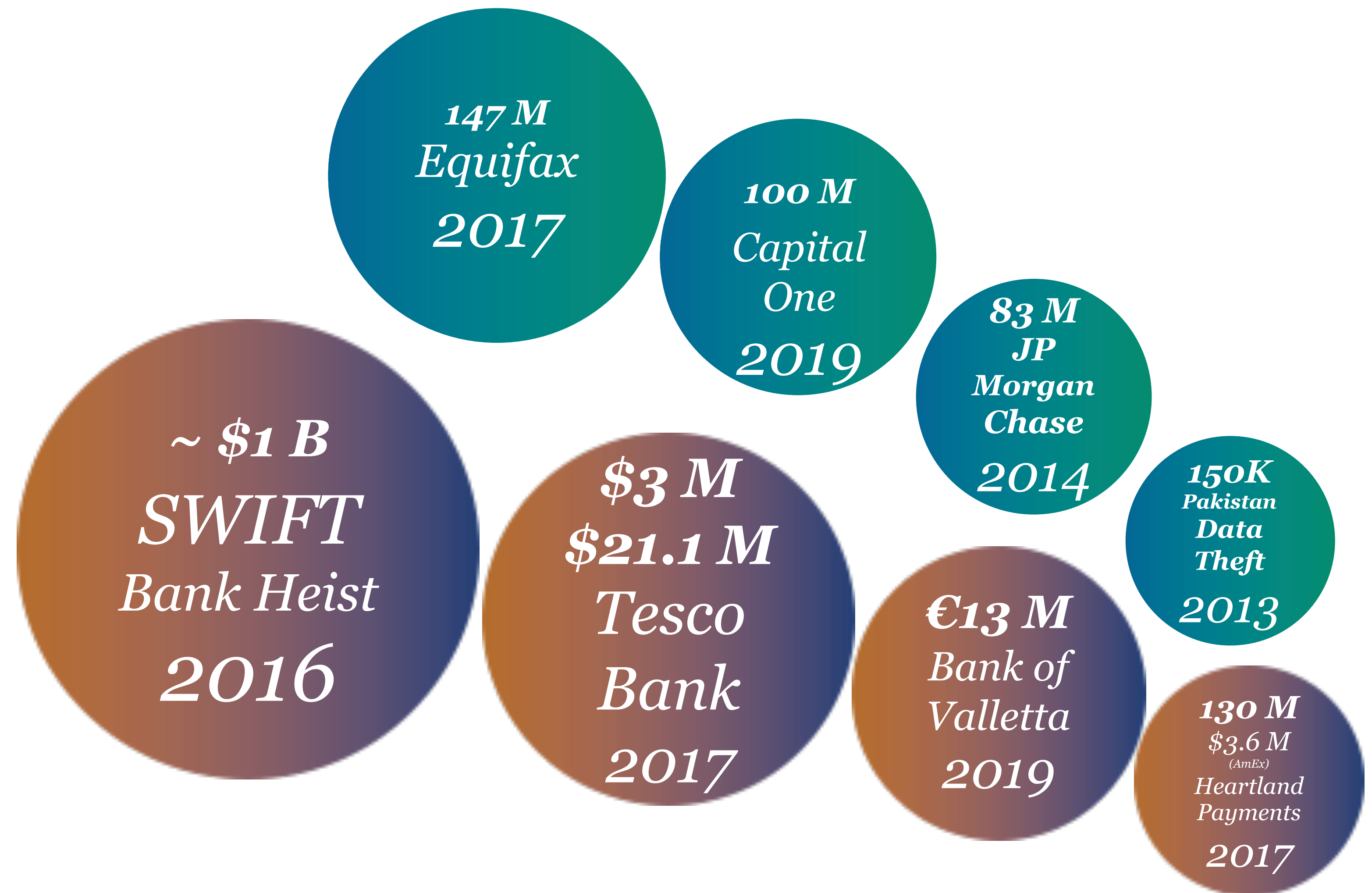
The shortest time taken to obtain total control over the banking network – 10 minutes.





# Few of the Biggest Cyber Attacks

## Finance Sector







24 JUN 2015

NEWS

# Finance Hit by 300 Times More Attacks Than Other Industries



Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster





Financial services firms are hit by security incidents a staggering 300 times more frequently than businesses in other industries, with attack patterns changing frequently to outwit IT pros, according to Websense.

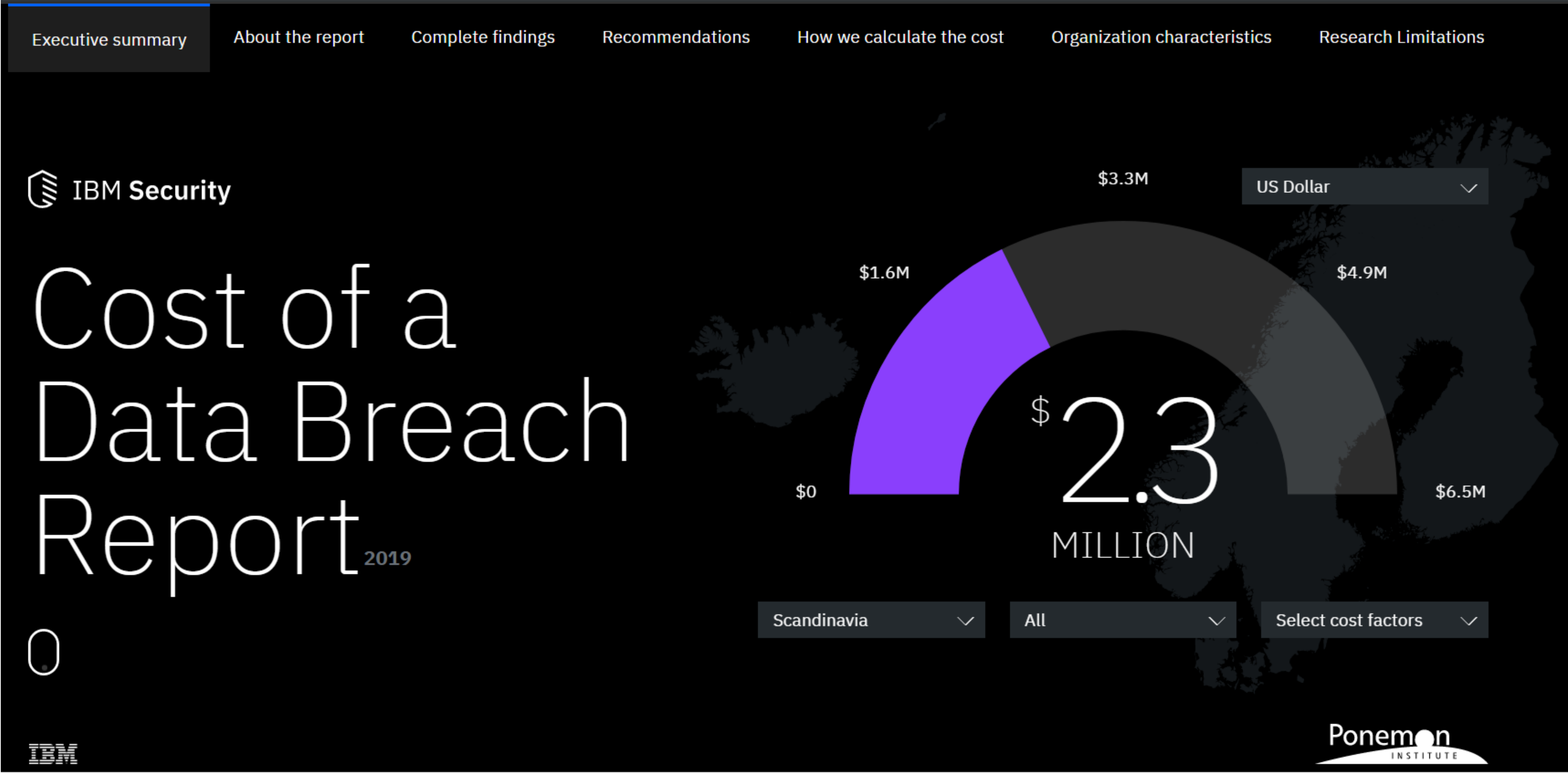




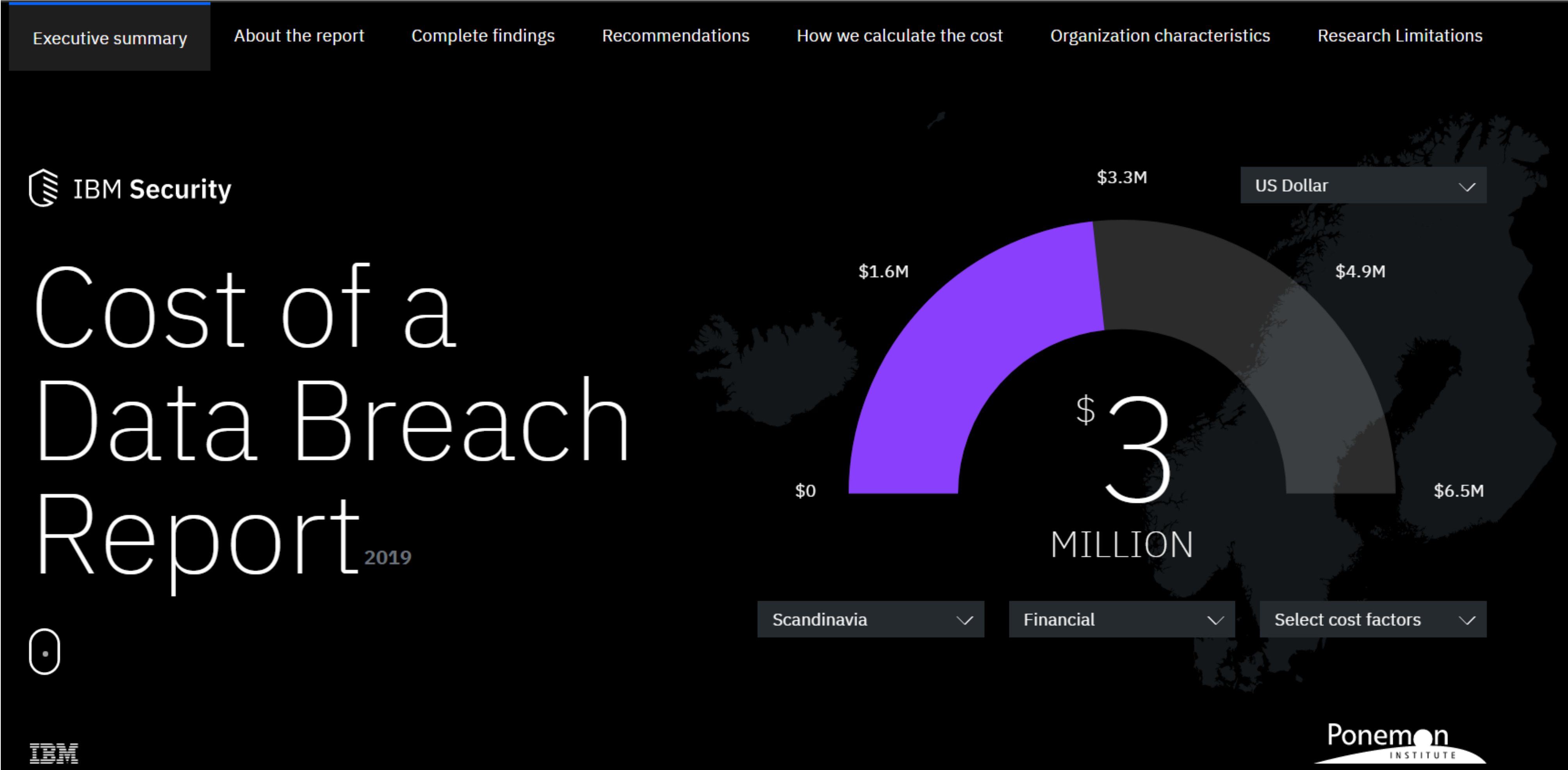
# Highest Industry Average Cost per record Scandinavia Finance Sector

Global Averages 		Scandinavia Averages 	
Average total cost of a data breach <b>\$3.92M</b>		Average total cost of a data breach <b>\$2.30M</b>	
Average size of a data breach <b>25,575 records</b>		Average size of a data breach <b>21,663 records</b>	
Cost per lost record <b>\$150</b>	Time to identify and contain a breach <b>279 days</b>	Cost per lost record <b>\$130</b>	Time to identify and contain a breach <b>299 days</b>
Highest country average cost of \$8.19 million <b>United States</b>	Highest industry average cost of \$6.45 million <b>Healthcare</b>	Country rank for total cost <b>12</b>	Highest industry average for cost per record <b>Financial</b>













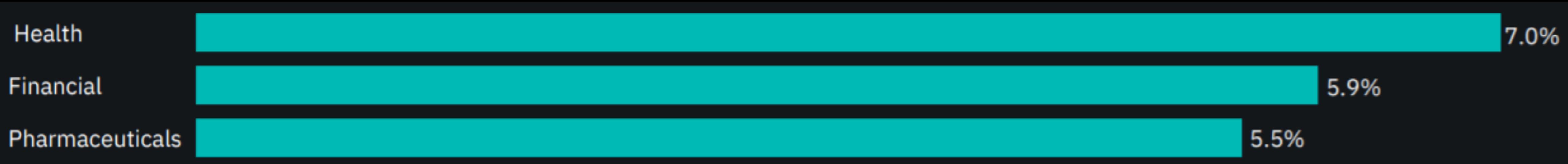
The global average customer turnover rate was 3.9 percent, an increase from last year's report of customer turnover rate of 3.4 percent.

3.9%

2019 abnormal customer turnover rate

3.4%

2018 abnormal customer turnover rate





147 M  
Equifax  
2017

**\$326M**  
*Equifax*  
since  
2017

During the year ended December 31, 2018, the Company recorded \$401.2 million of pre-tax expenses **related to the 2017 cybersecurity incident** and insurance recoveries of \$75.0 million for **net expenses of \$326.2 million.**

**\$575M**  
*Equifax*  
FTC  
2019





# Equifax's Data Breach Costs Hit \$1.4 Billion

Massive 2017 Breach Continues to Bite the Credit Reporting Giant's Bottom Line

Mathew J. Schwartz (euroinfosec) · May 13, 2019



Twitter

Facebook

LinkedIn

Credit Eligible

Get Permission



Credit reporting giant Equifax has spent nearly \$1.4 billion on cleanup costs as well as overhauling its information security program following its massive 2017 data breach.





**EQUIFAX®**



"It's one thing to defend against a hacker... But defending against the military arm of another government, in this case China, really raises the bar," Equifax CEO Mark Begor said about today's indictment.  
[cnb.cx/2UFVg6w](https://cnb.cx/2UFVg6w)







# Differentiator

Something that differentiates!  
Gives you competitive edge!





Not just a matter of if  
and when, but

how long?  
how much impact?  
how to contain?  
how to invest?  
how to continue?







# Business Differentiator Key Elements







# **1. Business Involvement**

## **2. Cyber Resilience**

### **3. Risk Quantification**





# Business Involvement



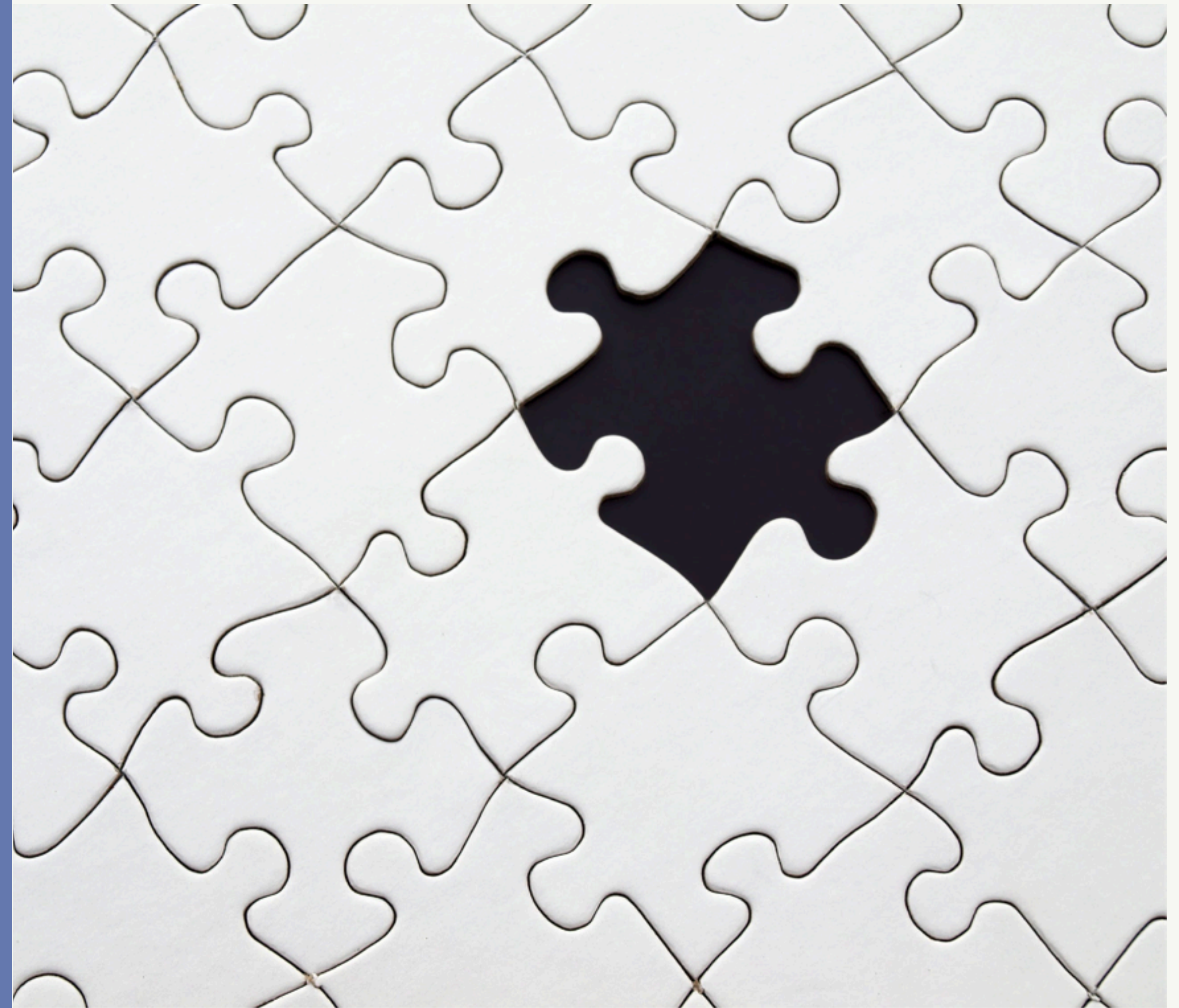
# 1. Business Involvement

All assessment of vulnerabilities and cyber risks require

a) context

b) and business involvement

to understand and connect the business and financial impacts.







# Cyber Resilience



## 2. Cyber Resilience

Cybersecurity + Business Resilience

Anticipate Chaos! Be Prepared!

Critical to understand the threat landscape and the cybersecurity risks you face

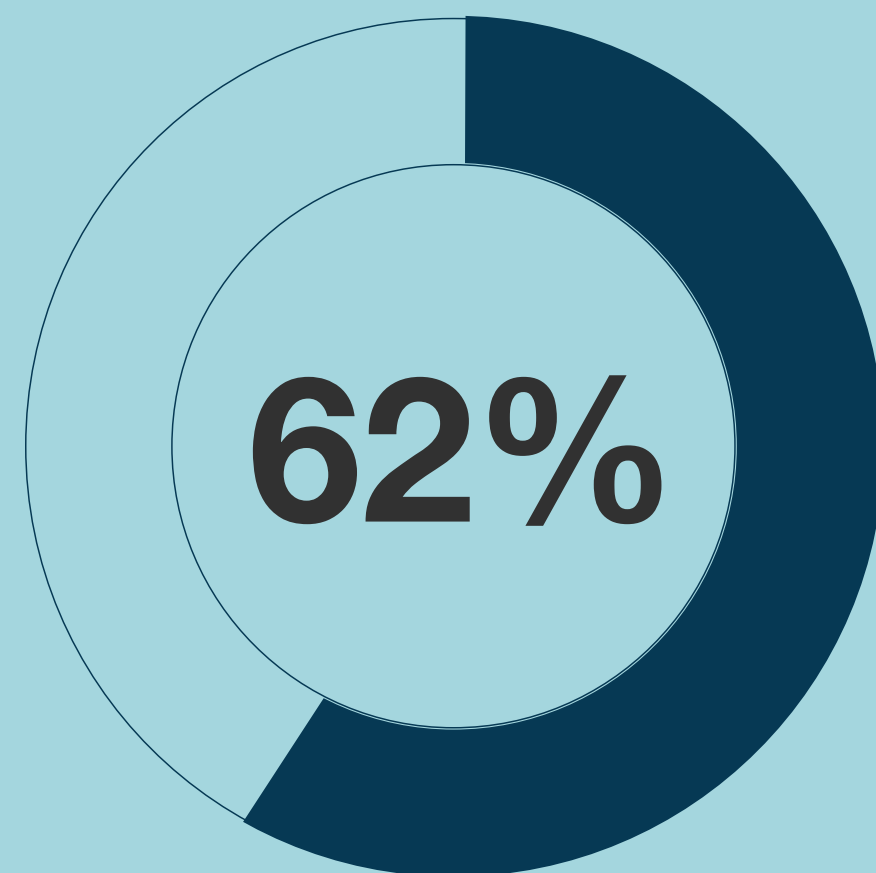
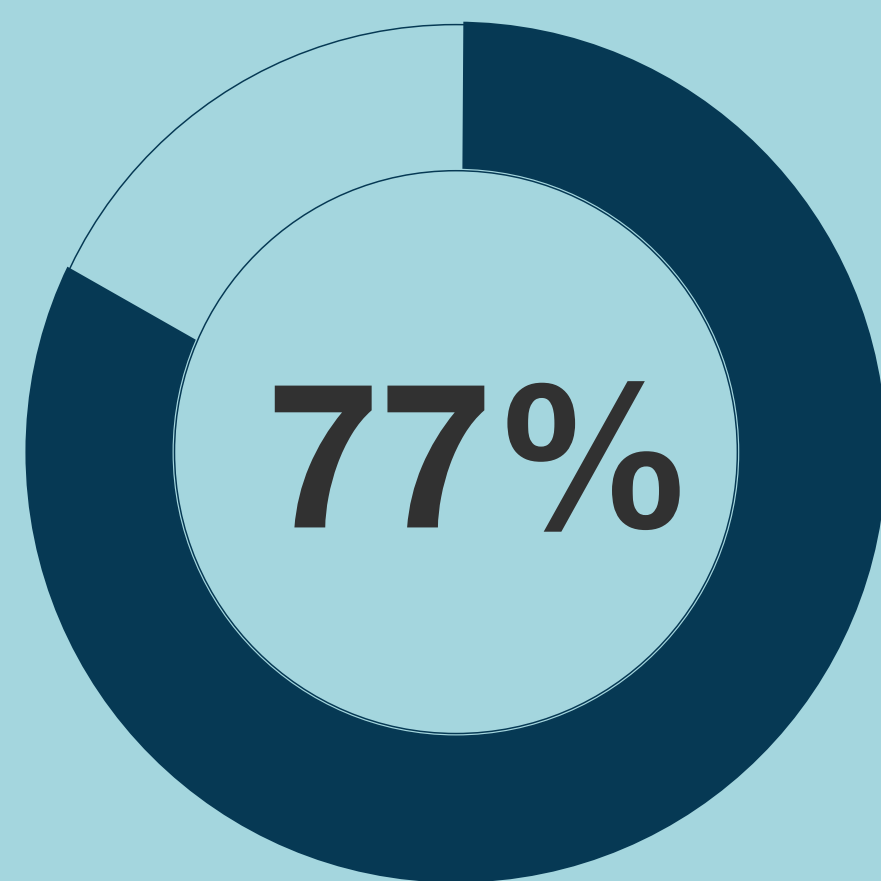
Resilience happens when you are better able to detect, contain and respond to cyber attacks, whilst shortening time required to be back to normal business operations.







## 2. Cyber Resilience



77 percent of firms surveyed lack proper cyber resilience plans

Only 44 percent of respondents believe their organizations' leaders recognize that enterprise risks affects cyber resilience

62 percent of respondents say risk assessment is a critical element to cyber resilience plans





# Cyber Resilience

**Anticipate Chaos!**  
**Be Prepared!**





# Risk Quantification





## 3. Risk Quantification

Financial estimation of a cyber risk including financial, business and reputational impact, in order to

- a) understand risk exposure
- b) ensure right security investment and risk management strategy.







The risk I took was calculated,  
.....but man, I am bad at math.



Financial Risk  
Management

Cyber Risk  
Management

Quantitative

Qualitative





## Bull's Eye



It's about balancing  
accuracy and precision!







**Cyber Risk  
Management:  
A part of  
Enterprise Risk  
Management**

**Clear and Well-  
Defined Risk  
Appetite and  
Tolerances**

**The True Cost  
of a Cyber  
Incident**

**Right  
Expertise.  
  
Right  
Competency.**





**Categorization**  
Key Scenarios  
and Key Cyber  
Risks

**Threat Factor**  
Capability and  
Motivation

**Monetary Loss**  
(Range of)  
Amount of loss  
with ca. 90%  
certainty

**Subjective BUT**  
**numeric**  
(amount or  
range)





1. Security governance and management with regards to Confidentiality, Integrity & Availability (CIA) across organization and integrated with the business.



2. Timely detection of cyber attacks and adequate level of cyber resilience within systems, services and business operations, to ensure protection of entire ecosystem.



3. Quantitative risk management to minimize impact on the business, treat cyber risks adequately, and to quantify organization's cyber resilience and security capabilities.





“In today’s digital landscape, cyber risk is not only an enterprise risk but also a systemic risk.”

Monica Verma, Chief Information Security Officer (CISO)  
Board Member, Cloud Security Alliance Norway