Developed and Hosted by

3rd CISO 360 CONGRESS 2019 Rome

PULSE CONFERENCES

Welcome and Thanks

Platinum

TELSTRA

Gold

Company85 accomplish more

SailPoint

CYBERARK

BITSIGHT

BARCLAY SIMPSON.

NOMINET

AGARI

ExtraHop Rise Above the Noise.

netwrix

DARKTRACE

zscaler

RISKIQ

OneTrust Privacy Management Software

proofpoint.

Silver

SOC PRIME SECURITY QUALITY CONTROL

Synack

Fidus INFORMATION SECURITY

CyberCyte

Bronze

CHECKMARX

Lunch Sponsor

IDECSI Enterprise Security

Panel Sponsors

GARRISON

avatao Learn to build secure software

NetClean.

Exhibition Sponsor

GURUCUL

Supporting Associations

(ISC)² OFFICIAL CHAPTER

ISACA Rome Chapter

3rd CISO 360 CONGRESS 2019 Rome

Chairman's Opening Global Risk Horizon

Marcus Alldrick

Former CISO, Lloyd's of London & Principal Senior Advisor Risk, Compliance (United Kingdom)

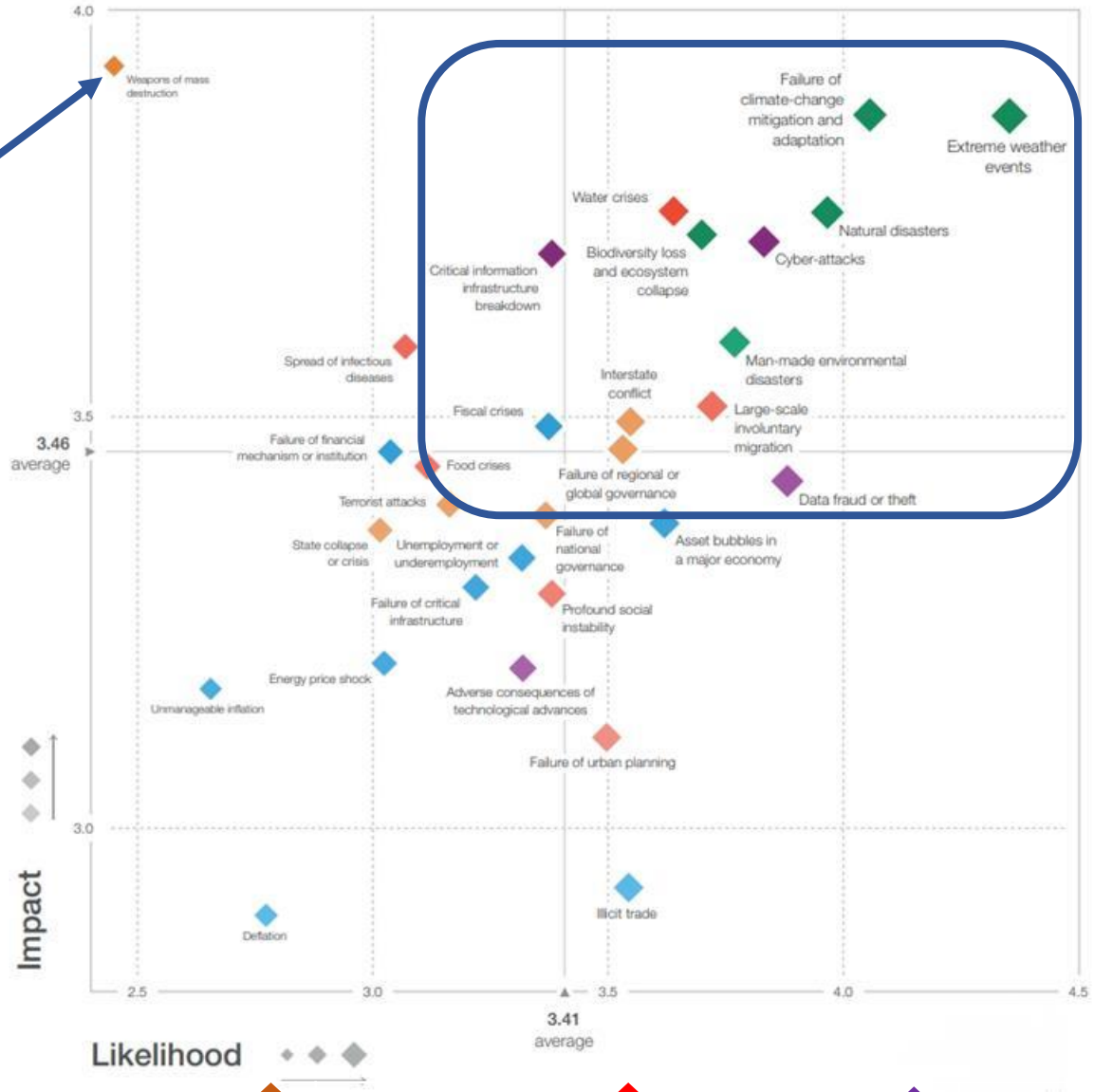
PULSE CONFERENCES

Global Risk Horizon 2019 and beyond

CISO 360 Congress 2019, Rome

The Global Risks Landscape 2019

Weapons of mass destruction



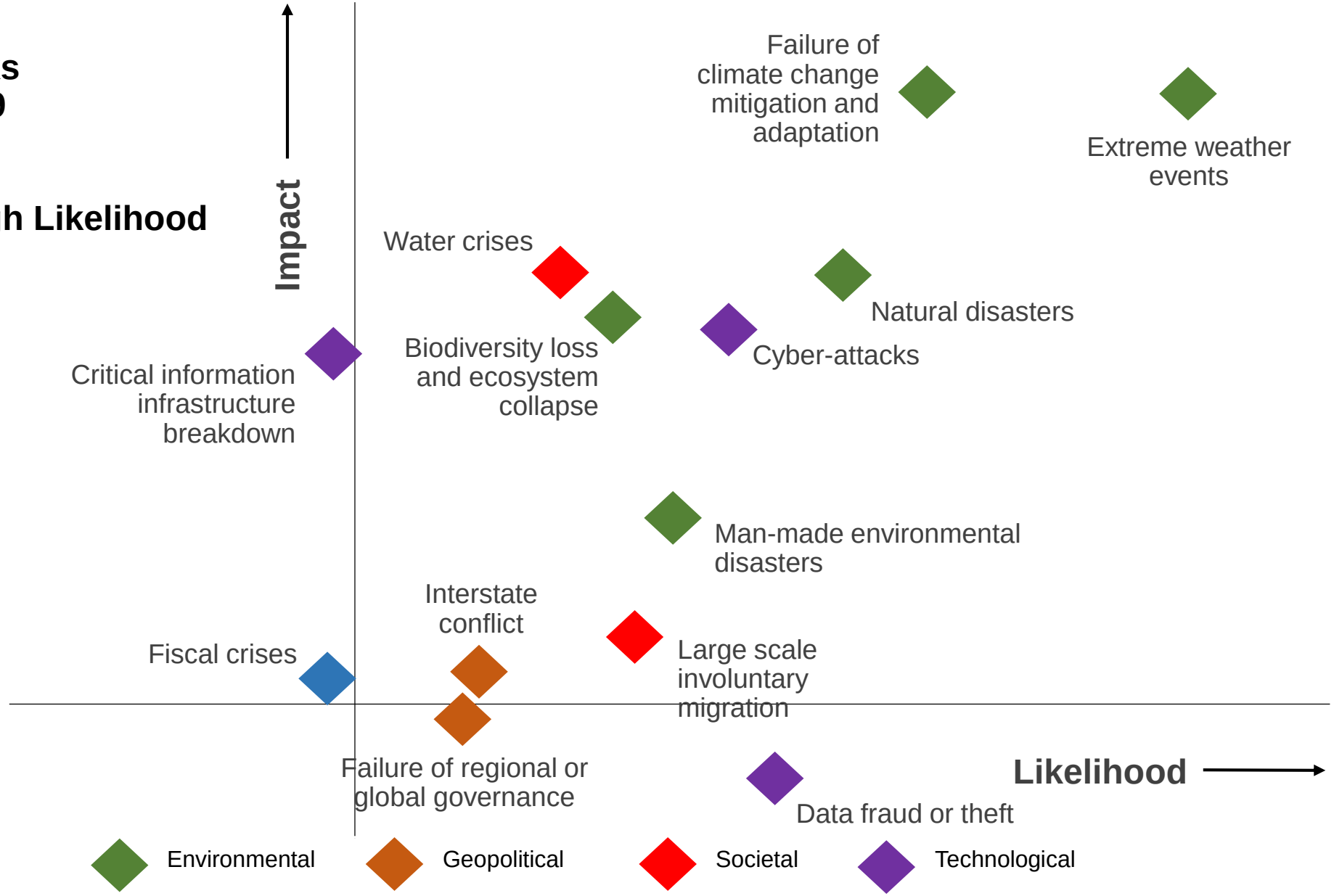
Key

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: *World Economic Forum The Global Risks Report 2019*

The Global Risks Landscape 2019

Focus on High Impact High Likelihood Quadrant



Source: *World Economic Forum The Global Risks Report 2019*

World's Biggest Data Breaches & Hacks

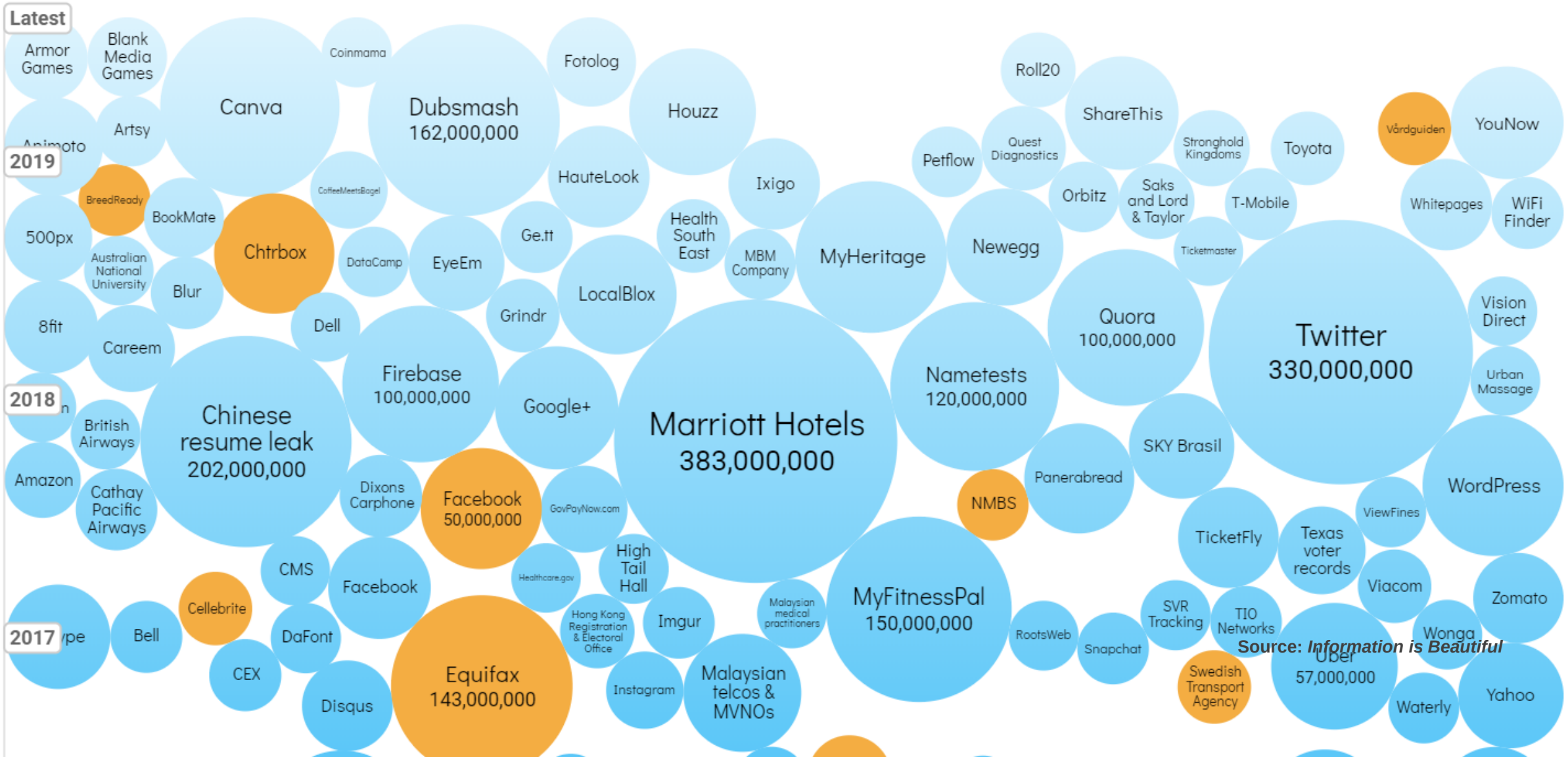
Select losses greater than 30,000 records

Last updated: 1 April 2019

interesting story

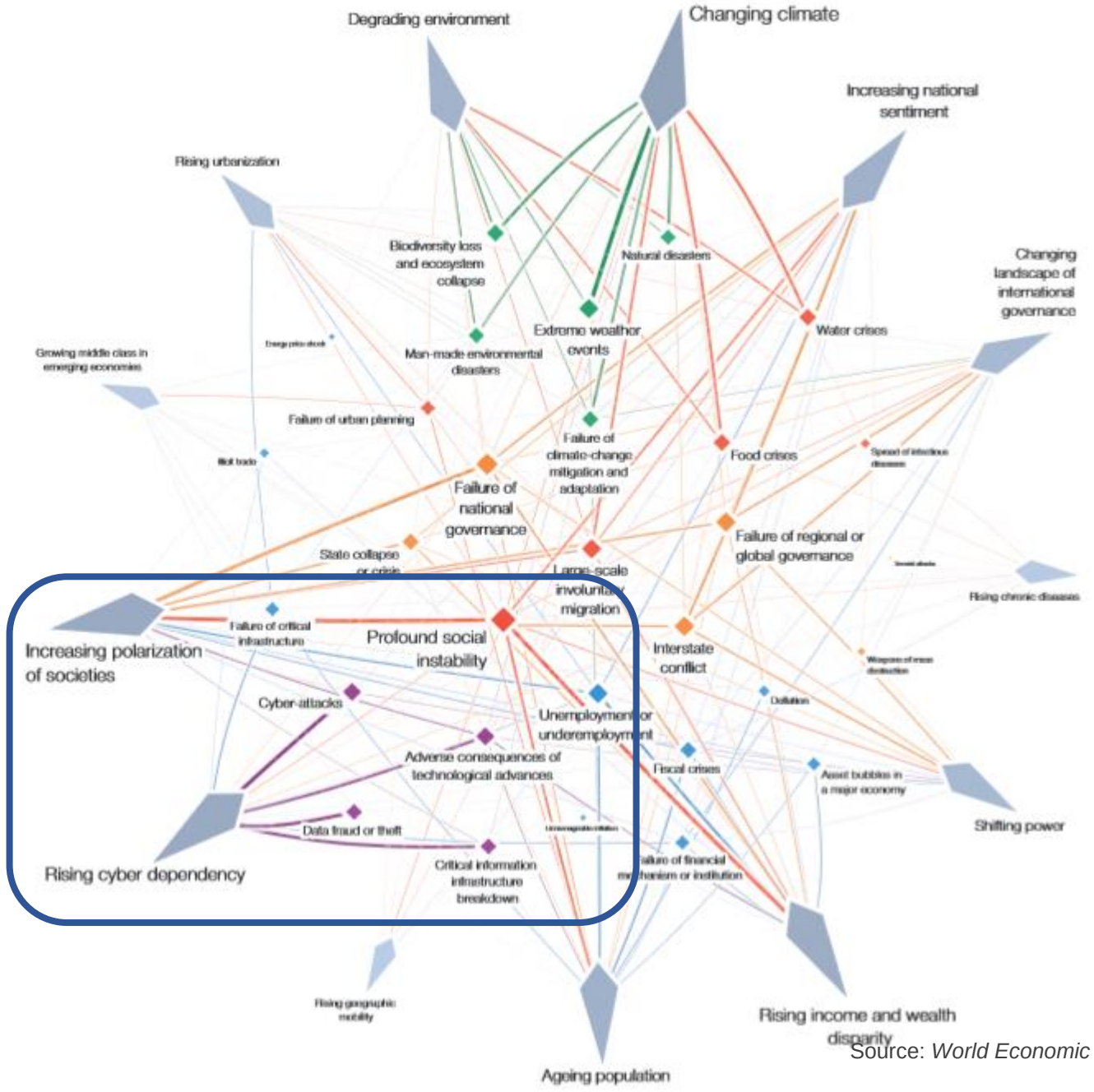
Filter Colour YEAR DATA SENSITIVITY

2009 2019 Search...



Source: *Information is Beautiful*

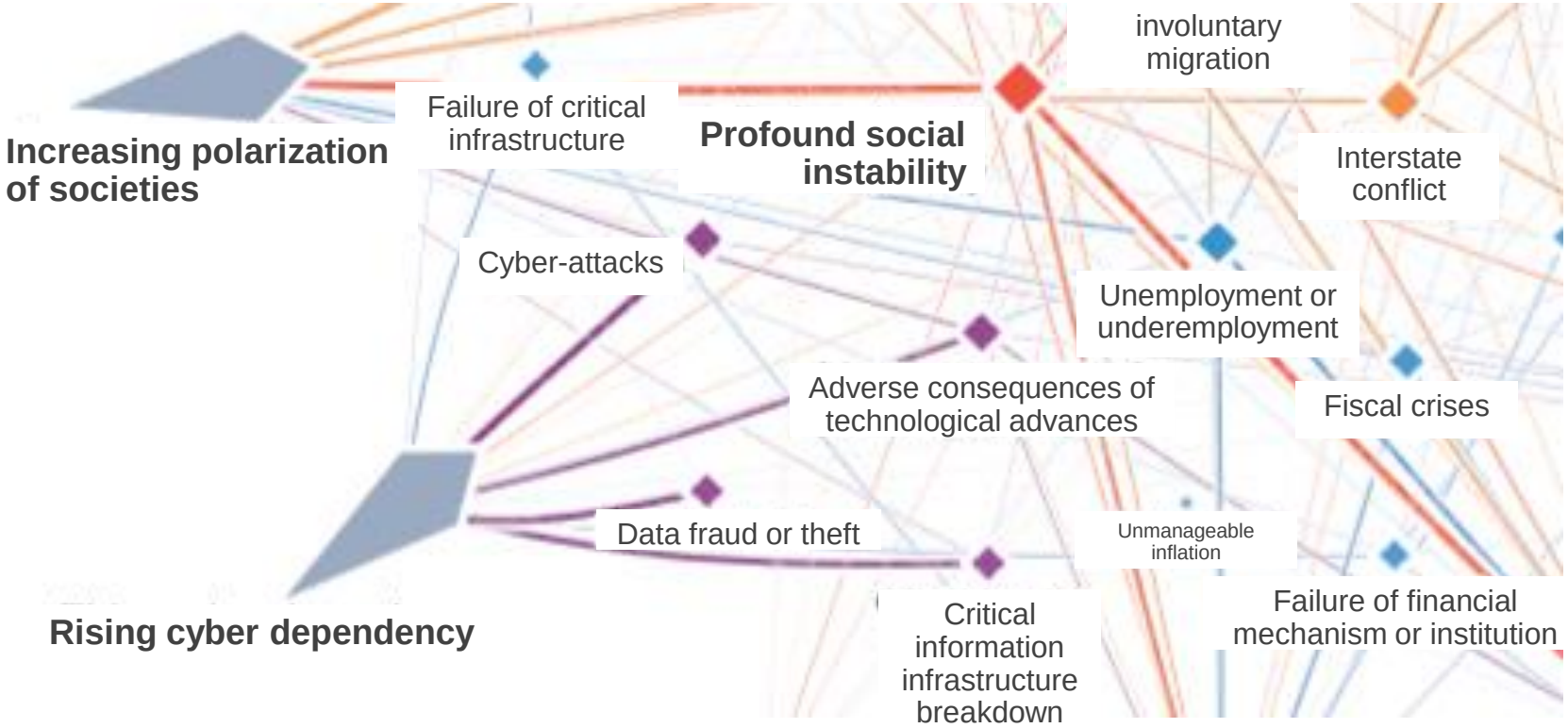
The Risks-Trends Interconnections Map 2019



Source: *World Economic Forum The Global Risks Report 2019*

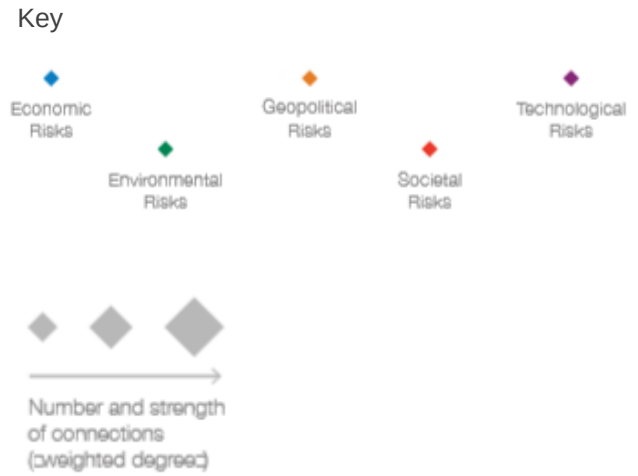
The Risks-Trends Interconnections Map 2019

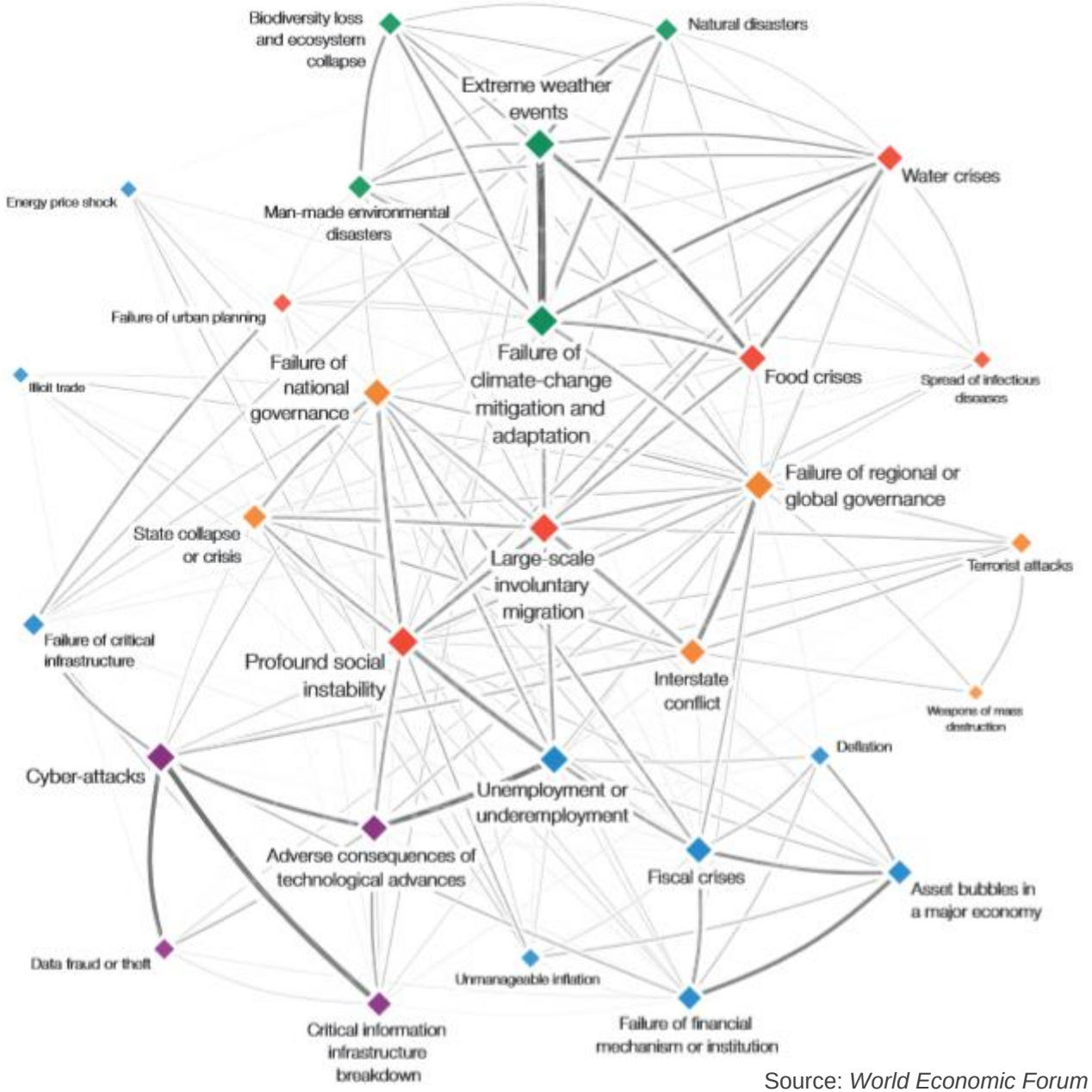
Focus on Rising cyber dependency



Source: *World Economic Forum The Global Risks Report 2019*

The Global Risks Interconnections Map 2019





Source: *World Economic Forum The Global Risks Report 2018*

The Evolving Risks Landscapes, 2009 to 2019

Top 5 Global Risks in terms of Likelihood

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Storm and cyclones	Severe income disparity	Severe income disparity	Income disparity	Interstate conflict	Largescale involuntary migration	Extreme weather events	Extreme weather events	Extreme weather events
2nd	Slowing Chinese economy	Slowing Chinese economy	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events	Extreme weather events	Largescale involuntary migration	Natural disasters	Failure of climate-change mitigation
3rd	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemploy-ment and under-employment	Failure of national governance	Failure of climate-change mitigation	Major natural disasters	Cyber-attacks	Natural disasters
4th	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber-attacks	Water supply crisis	Climate change	State collapse or crisis	Interstate conflict	Large-scale terrorist attacks	Data fraud or theft	Data fraud or theft
5th	Retrench-ment from globalization	Global governance gaps	Climate change	Water supply crises	Manage-ment of population	Cyber-attacks	Unemploy-ment and under-employment	Major natural catastrophes	Data fraud or theft	Failure of climate-change mitigation	Cyber-attacks

Key Economic | Environmental | Geopolitical | Societal | Technological

Source: *World Economic Forum The Global Risks Report 2019*

The Evolving Risks Landscapes, 2009 to 2019

Top 5 Global Risks in terms of Impact

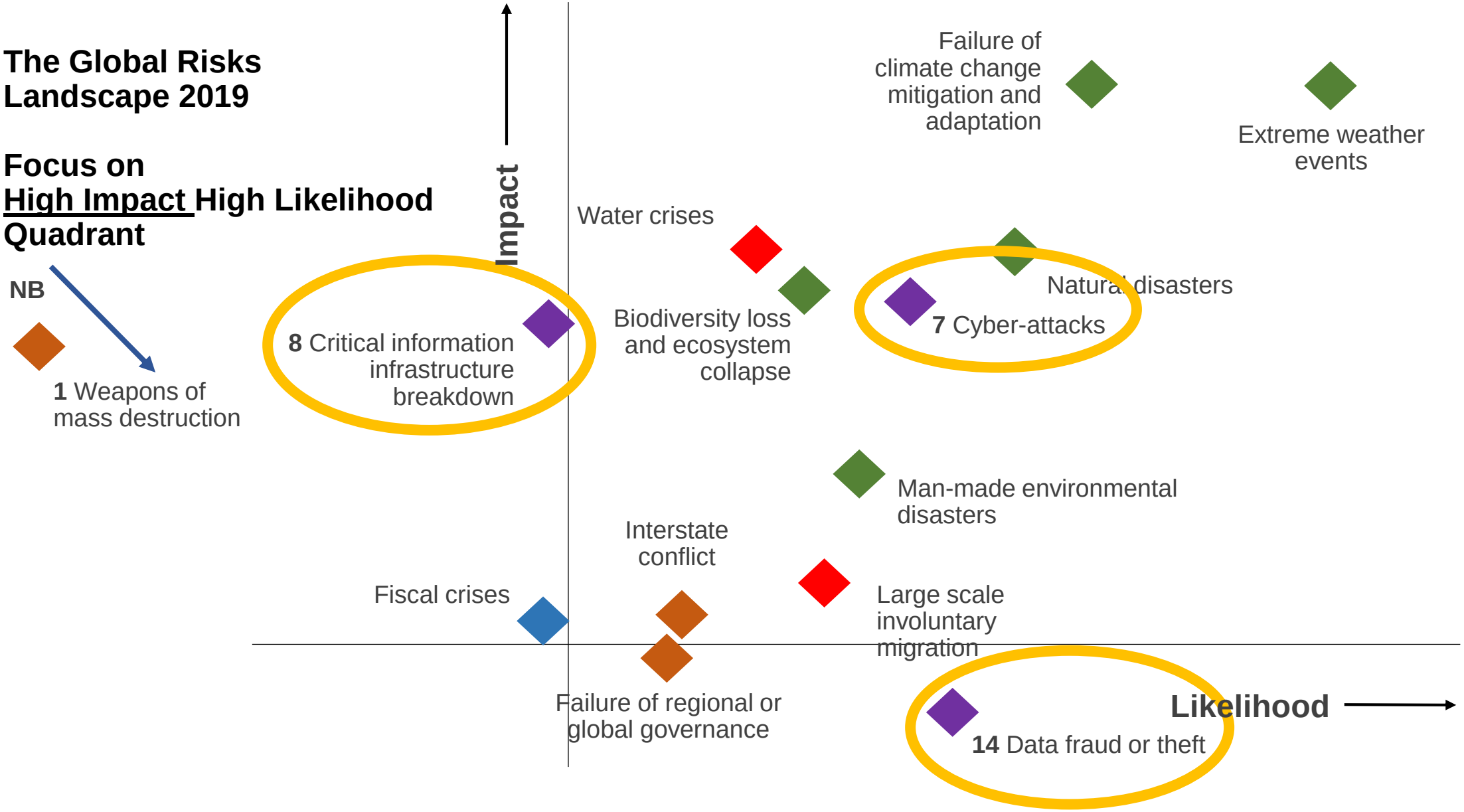
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Fiscal crises	Major systemic financial failure	Major systemic financial failure	Fiscal crises	Water crises	Failure of climate change mitigation	Weapons of mass destruction	Weapons of mass disruption	Weapons of mass disruption
2nd	Retrench-ment from globalization	Retrench-ment from globalization	Climate change	Water supply crises	Water supply crises	Climate change	Rapid and massive spread of infectious diseases	Weapons of mass destruction	Extreme weather events	Extreme weather events	Failure of climate-change mitigation
3rd	Oil and gas price spike	Oil price spikes	Geopolitical conflict	Food shortage crises	Chronic fiscal imbalances	Water crises	Weapons of mass destruction	Water crises	Water crises	Natural disasters	Extreme weather events
4th	Chronic disease	Chronic disease	Asset price collapse	Chronic fiscal imbalances	Diffusion of weapons of mass destruction	Unemploy-ment and under-employment	Interstate conflict	Large-scale involuntary migration	Major natural disasters	Failure of climate-change mitigation	Water crises
5th	Fiscal crises	Fiscal crises	Extreme energy price volatility	Extreme volatility in energy and agri prices	Failure of climate-change mitigation	Critical information infrastructure breakdown	Failure of climate-change mitigation	Severe energy price shock	Failure of climate-change mitigation	Water crises	Natural disasters

Key Economic | Environmental | Geopolitical | Societal | Technological

Source: *World Economic Forum The Global Risks Report 2019*

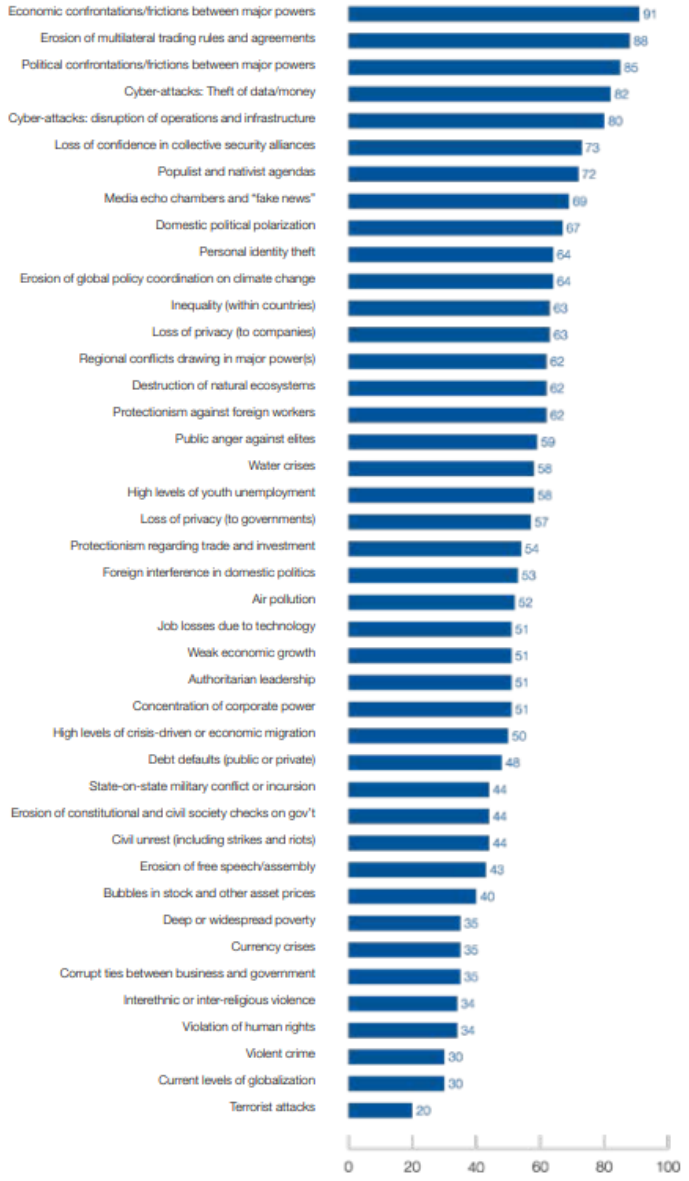
The Global Risks Landscape 2019

Focus on High Impact High Likelihood Quadrant

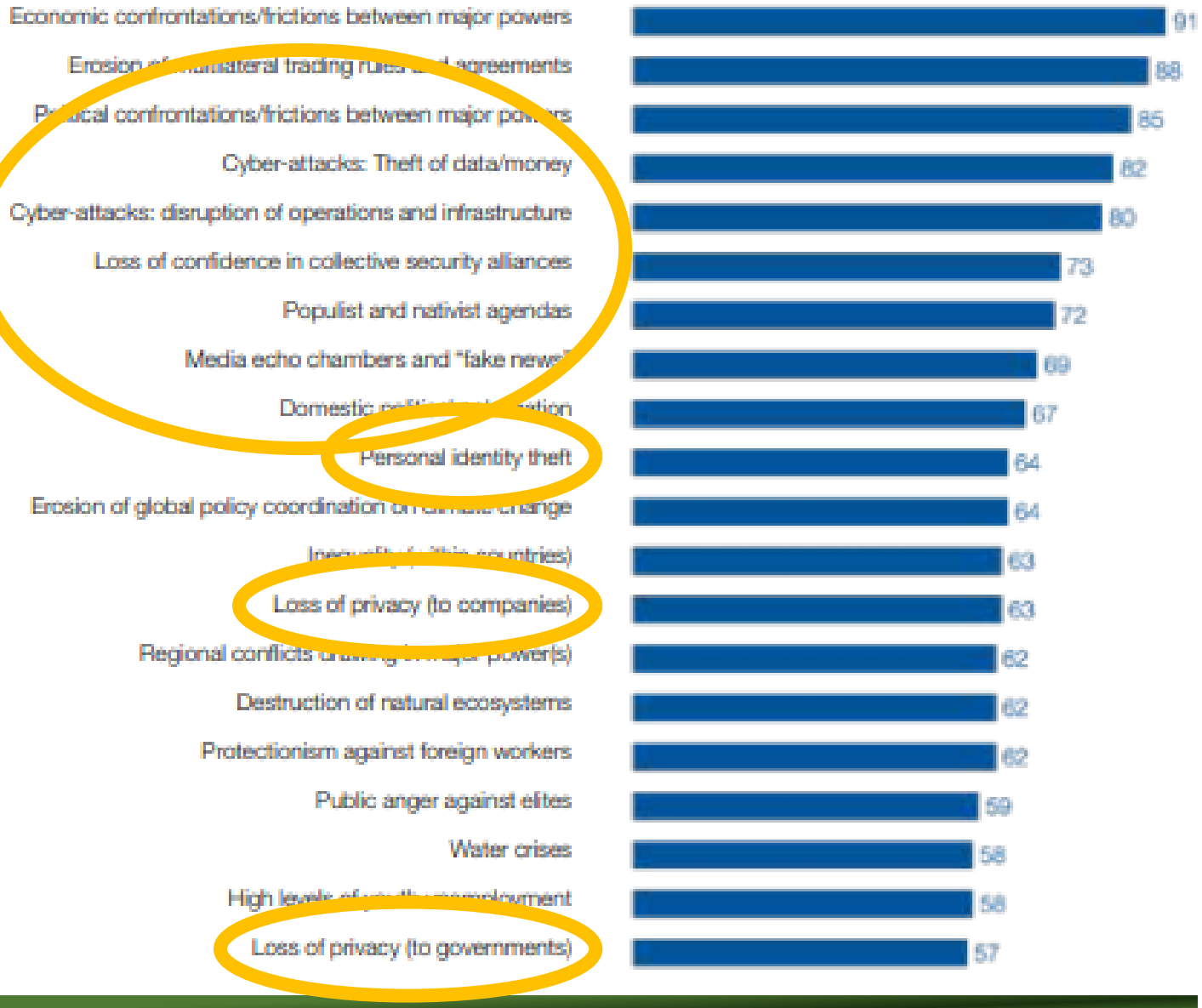


Source: *World Economic Forum The Global Risks Report 2019*

Short-Term Risk Outlook



Top 20 Short-Term Risks



Key conclusions

- Addressing target risks has resulted in numerous countervailing (unintended) risks with strong cyber implications
- Geopolitical volatility is a strong contributor to the Global Economic Downturn with real GDP growth expected to decelerate, debt burden to increase and low-income countries increasingly at high risk of debt distress
- Further exacerbated by increasing geoeconomic tensions resulting in divergence, collectively restricting global cooperation on a number of global challenges including cyber with systemic risks possibly increasing
- Weakening multilateralism resulting in reduced effectiveness of security alliances and protection of the global commons
- State sponsored/enabled/conducted cyber attacks will continue in response to sanctions and military conflict exacerbated by nation state unilateralism and commensurate reduction in governmental and organisational cooperation
- A primary directly manageable operational risk is clearly cyber related (*Cyber-attacks / Critical information infrastructure breakdown / Data fraud or theft*) which C-Suites and Boards would be foolhardy to ignore
- Fake news, identity theft, loss of privacy to companies and governments expected to increase due to deepening integration of digital technologies and use of AI to engineer more potent cyber-attacks
- Hardware and software vulnerabilities in critical technological infrastructure increasing concern resulting in increasing focus on supply chain risks at national level to protect critical infrastructure, also reflected at the organisational level
- Actual occurrences, volumes and impact of *Cyber-attacks* and *Data fraud or theft* possibly higher than indicated due to lax cybersecurity protocols and lack of transparency on reporting incidents and direct and consequential impact
- Despite this Cyber budgets and spend will be challenged: more for less with increased integration, consolidation and monitoring with increasing indications to monetise cyber security and provide increased tangible ROI
- Other, notably Environmental, risks cannot be ignored due to their direct, consequential operational & reputational risks.

Thank you

Bramwell
buckingham

3rd CISO 360 CONGRESS 2019 Rome

OPENING Keynote Host Nation

Dr. Stefano Zanero

Associate Professor, University of Milan (Italy)

PULSE CONFERENCES

POLITECNICO DI MILANO





Securing Cyber-Physical Systems: moving beyond fear

Stefano Zanero, PhD
Associate Professor, Politecnico di Milano

Welcome to the security circus!

We all like to see the attractions

We all like to see the attractions

We all like to see the attractions

And what are the attractions, really?

- Our conferences reward **attack research**
- Because we are hackers at heart and we enjoy the **beauty** of many of these hacks, their skill and their ingenuity
- But you may have realized by now that we are not on IRC in our hacker crews anymore
- We are on the top frontpage news
- Our findings **impact the public perception**

Why is this the case with cyber-physical systems in particular?

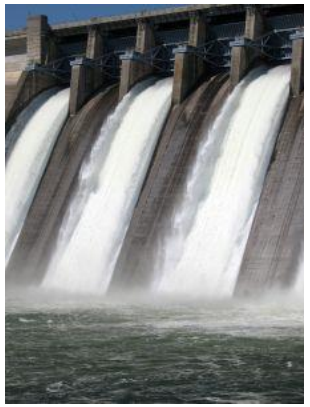
- They are systems that people **see** and can immediately perceive as **relevant**

The great cyberfear is spreading

"… potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: *no more electricity or water* at home, *rail and plane accidents, hospitals out of service*"

Viviane Reding

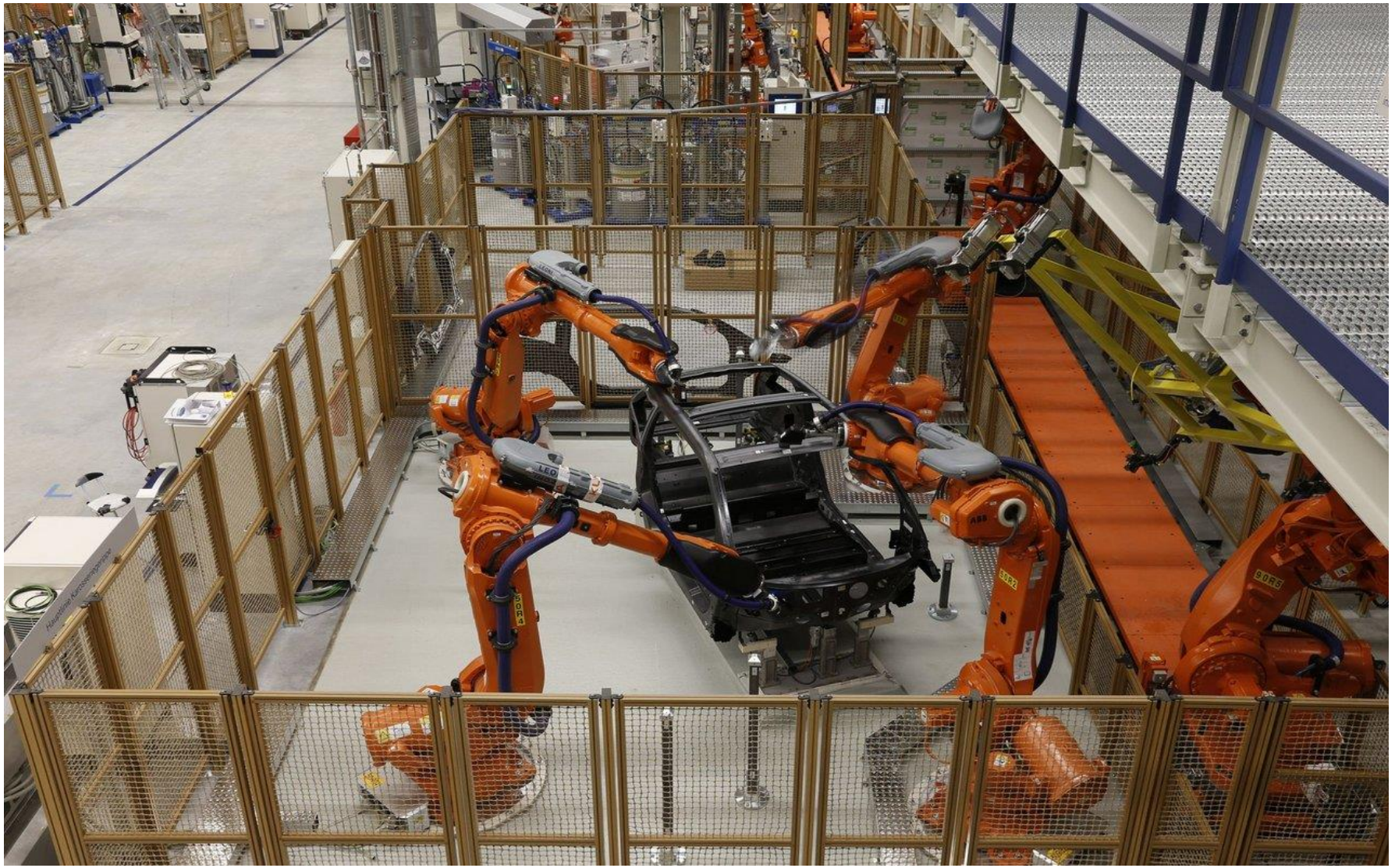
VP of European Commission (at time of delivering these remarks)



Why is this the case with cyber-physical systems in particular?

- They are systems that people **see** and can immediately perceive as **relevant**
- They are systems with **safety** constraints which may involve danger for **human life**

For instance, industrial robots...



… are getting out of their cages

Why is this the case with cyber-physical systems in particular?

- They are systems that people **see** and can immediately perceive as **relevant**
- They are systems with **safety** constraints which may involve danger for **human life**
- They are systems that are becoming more and more reliant on automation (think: autonomous vehicles!)

Automation has always evoked fear

We can’t just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**

Words of wisdom

"Bruce Schneier asked a cogent, first-principles question: Are vulnerabilities in software dense or sparse? If they are sparse, then every vulnerability you find and fix meaningfully lowers the number of vulnerabilities that are extant. If they are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it."

Dan Geer

We can’t just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**
- **We are not going to solve anything by just squashing one vulnerability at a time!**

Words of wisdom

A flaw that Brad Spengler […] has been incessantly pointing out for years [is] that **bugs don't matter**. Bugs are irrelevant. Yet our industry is fatally focused on what is essentially vulnerability masturbation. [...]

And it's all bullshit. If you care about security that is. [...]

"But to stop exploitation you have to understand it!". Sure. But here's an inconvenient truth. **You are not going to stop exploitation. Ever.**

So if you truly, deeply, honestly care about security. Step away from exploit development. All you're doing is ducking punches that you knew were coming. It is moot. It is not going to stop anyone from getting into anything, it's just closing off a singular route.

But if you care about systemic security […] **don't chase and fix vulnerabilities, […] design a system around fundamentally stopping routes of impact.**

Containment is the name of the game. Not prevention. The compromise is inevitable and the routes are legion. It is going to happen.

Bas Alberts

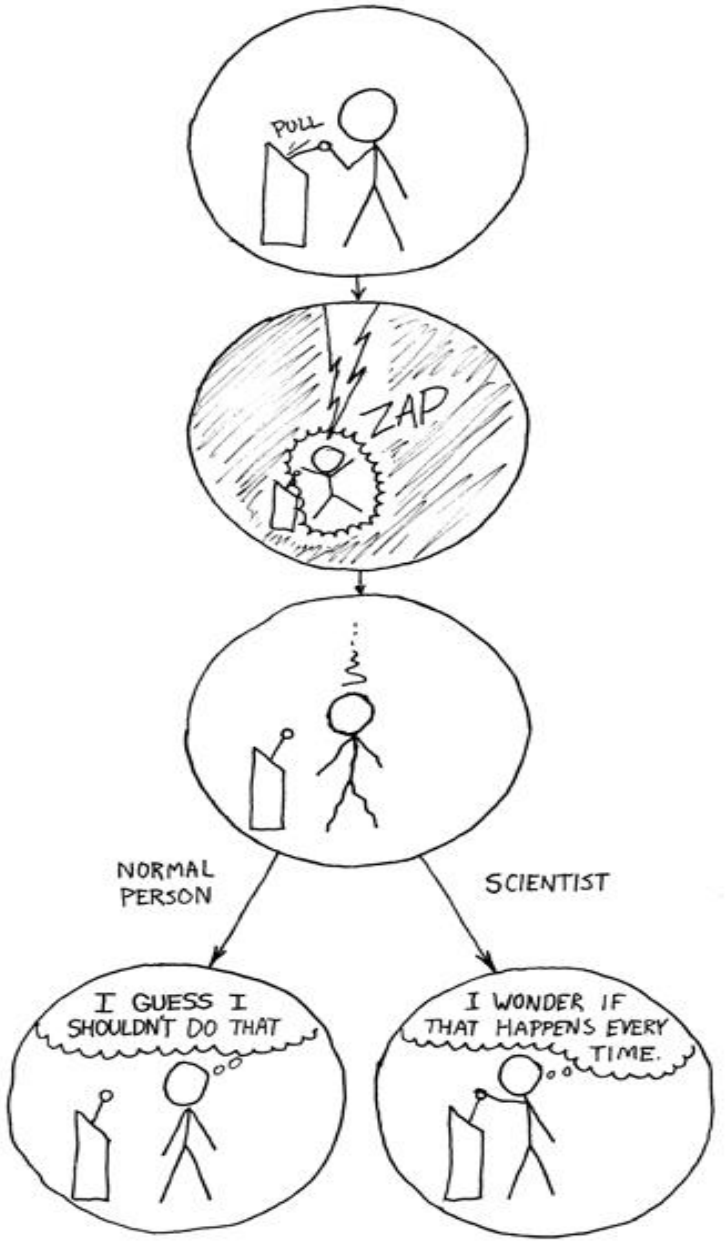
We can’t just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**
- **We are not going to solve anything by just squashing one vulnerability at a time!**
- In the specific case of CPS we need to **restore confidence** in the public and in our colleagues in other areas of the profession

Questions?

- Thank you for your attention!
- You can reach me at stefano.zanero@polimi.it
- Or just tweet @raistolo

Disclaimer: none of these materials, if posted without a video of the talk, should be construed to be a criticism of the specific research I used as examples.



3rd CISO 360 CONGRESS 2019 Rome

OPENING KEYNOTE Risk-taking and decision-making

Caspar Berry
Professional Poker Player

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

EU report highlights What are the top two current security challenges for organisations globally?

Joel Stradling

Research Director, GlobalData on Behalf of Telstra

PULSE CONFERENCES

Industry Insights and Key Findings from Telstra Security Report 2019

June 19, 2019

Joel Stradling
Research Director, GlobalData

TELSTRA

Agenda

- Trends and Observations
- Findings from the Telstra 2019 Security Report
- Recommendations

Enterprise Technology Drivers

Know the Enemy

- A new supply chain is in existence
- There is no discrimination – small businesses can become victims right up to large enterprise and government

The Cybercriminal Ecosystem

SCADA Industrial Control Meets the Internet

- Critical infrastructure management is increasingly on-line
- Physical device security is poorly integrated with IT and network
- Businesses and governments are increasingly dependent on automated IT systems

Key Findings from the Telstra 2019 Report

of European businesses were interrupted by a breach last year

say they have had breaches go undetected

of European businesses experiences a ransomware incident within the past year

experiencing one ransomware incident per quarter

Breach detection and response

In the worst-case scenario, you have around 1 minute to detect, 10 minutes to contain and 60 minutes to remediate a potential ‘’state-sponsored’’ attack. [i]

In Telstra Security report, 1 in 4 respondents reported that less than 10 per cent of breaches were undetected. Nearly 1 in 3 organisations (30%) estimate that breaches go undetected more than 40 % of the time.

24% of organisations surveyed take weeks, months or years on average to detect a security incident and breach

[i] 2019 CrowdStrike Global Threat Report

Human behaviour incidents

At least **30%** of European respondents reported monthly or weekly brute force hacking, malicious insider and employee human error incidents in 2018.

Employee human error was most prevalent overall, with **88%** of European respondents reporting at least one incident in the last 12 months.

26% identified accidental insider acts as the greatest risk to their organisation’s IT security.

Recommendations

- Reduce attack surface - new concepts to consider: the ‘app is a network’ – ‘the network is a computer’
- Zero-trust
- Security that is intrinsic to applications plus more prevention; proactive as well as reactive
- Executive and C-level involvement and security ingrained throughout an organization
- Training people and internal programs to help avoid for example ‘accidental insider’ breaches
- DevSecOps

Thank you

TELSTRA

3rd CISO 360 CONGRESS 2019 Rome

Unique Keynote What can exercises in future-thinking tell us about the cybersecurity and international diplomacy challenges that we need to prepare for?

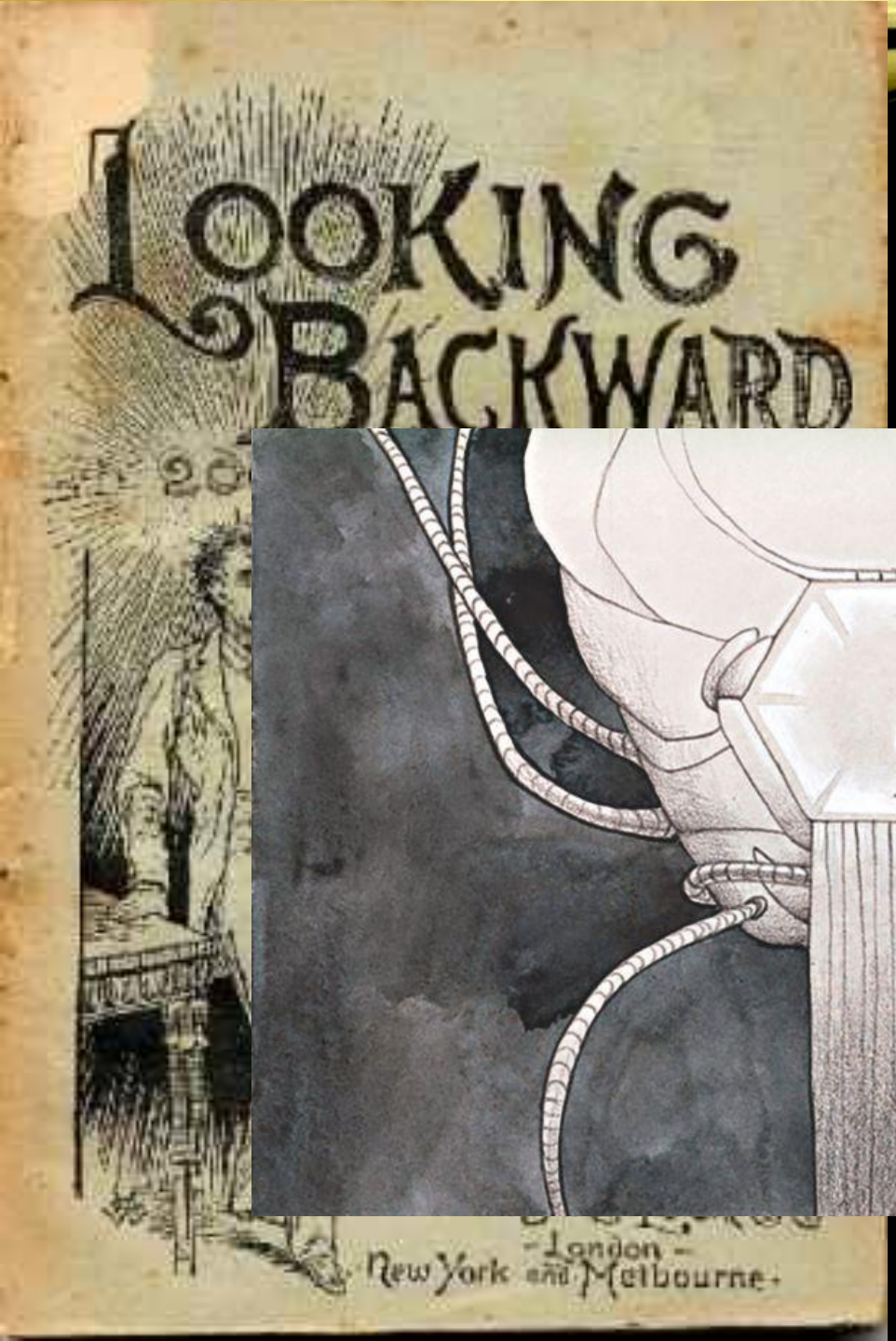
Dr. Victoria Baines
Visiting Associate, **Oxford Internet Institute** (UK)

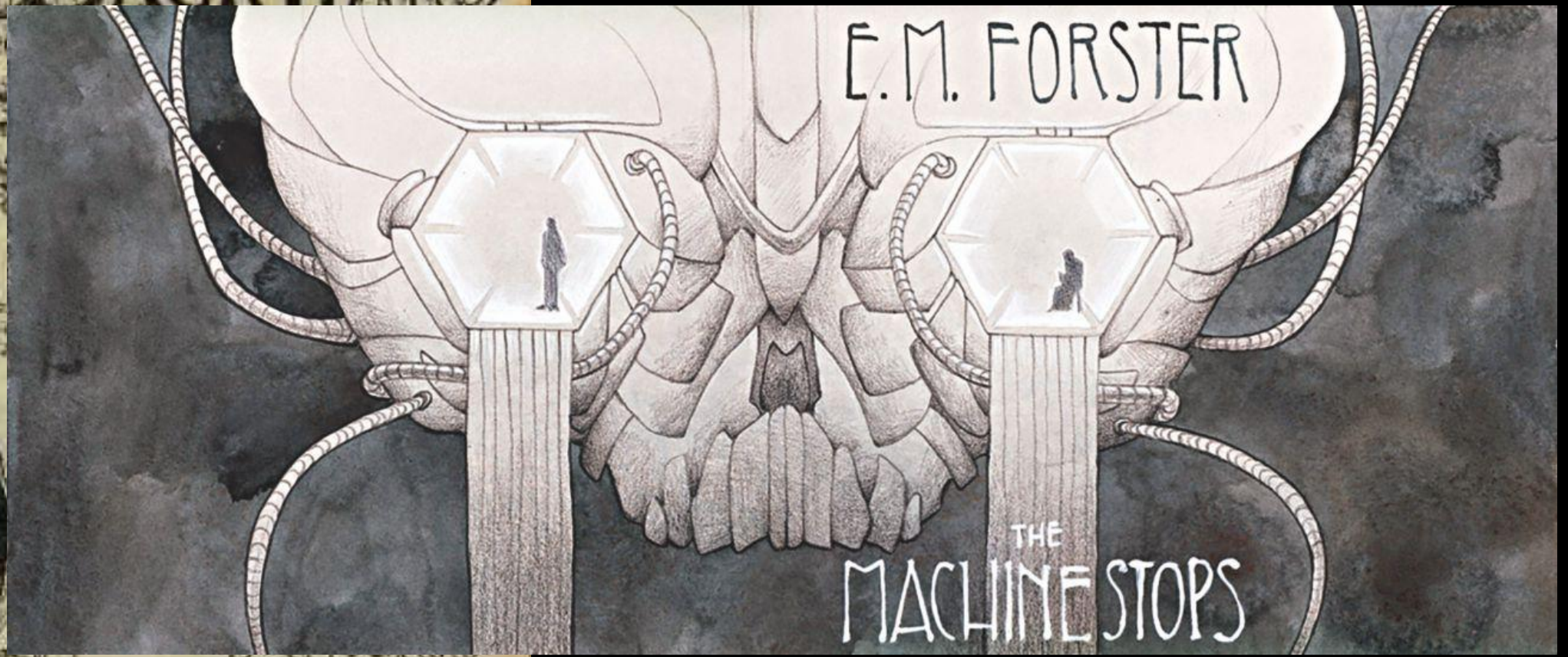
PULSE CONFERENCES

PREDICTING THE FUTURE OF CYBERSECURITY

Vic Baines, CISO 360 2019

THE BUSINESS OF PREDICTION





skynet
Belgacom

SKYNET
CYBERDYNE SYSTEMS CORPORATION

LIFE IMITATES ART

TESLASUIT

Ultimate tech in Smart Clothing

Development Kit

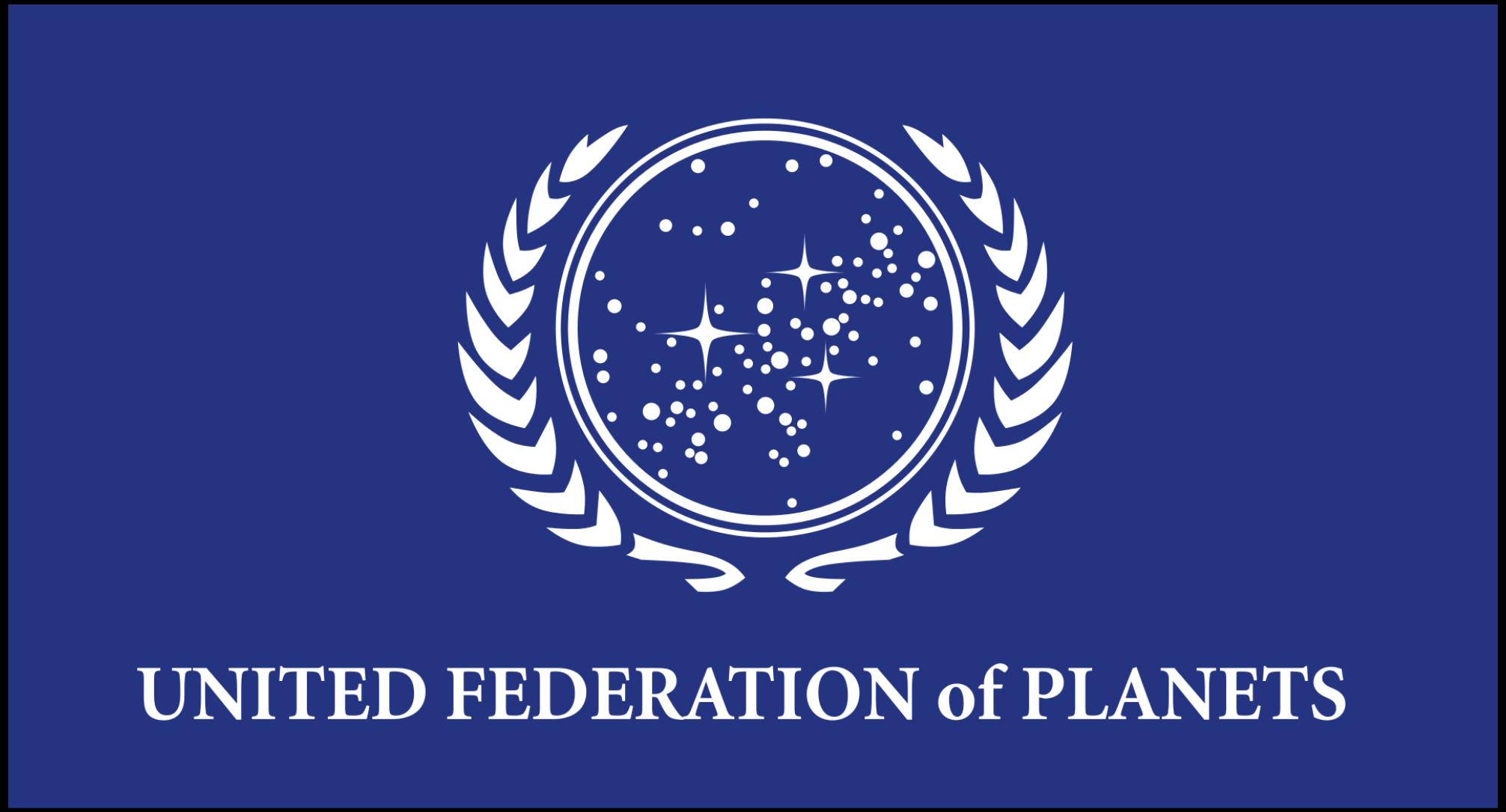
The world's first fully integrated smart clothing apparel with Haptic Feedback, Motion Capture, Climate Control and Biometric Feedback systems.

Whether you are a game developer, arcade owner or enterprise representative - we have a solution for you.

GET IN TOUCH

CYBERSECURITY FUTURES

WORLD GOVERNMENT



UNITED NATIONS?

"Episodes of cyber warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it."

UNITED NATIONS?

"I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack to destroy military capacity... and paralyse basic infrastructure such as the electric networks."

WHY IT MATTERS

- IDEOLOGICAL/POLITICAL DIFFERENCES IMPACT ON THE BUSINESS COMMUNITY
- GROWING PUBLIC INTEREST IN COMPANIES' SECURITY
- GROWING INTEREST IN COMPANIES' ASSISTANCE TO GOVERNMENTS
- BLURRING OF KINETIC AND CYBER WARFARE
- THE PROPAGANDA WAR HAS FAR-REACHING EFFECTS
- INCREASINGLY DIFFICULT TO FIND 'UNBLEMISHED' EXPERTS
- BALKANISATION VS. INTERNATIONAL CONSENSUS


MOON PATROL
XT-978

3rd CISO 360 CONGRESS 2019 Rome

Keynote and Practical Use Case Stories Using AI to counter the next generation of cyber-threats

---

Mariana Pereira
Director, Darktrace

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

4 BIG QUESTIONS What is technology's current emerging role in international diplomacy? Predictions and trade-offs

---

Chaired by: Lady Olga Maitland, Chairman, Copenhagen Compliance, Founder, Defence and Security Forum (UK)
Joined by: Dr. Victoria Baines, Visiting Associate, Oxford Internet Institute (UK)
Prof. Ing. Claudio Cilli, Dipartimento di Informatica, Università degli Studi di Roma "La Sapienza" and President, ISACA Rome Chapter (Italy)
Paul Brucciani, Head of Commercial Business Development, UK, Garrison Technology
Gadi Evron, Chairman of the Board, Israeli CERT (IL-CERT) (Israel)
Tim Varkalis, Group Security - Threat Intelligence Lead, AXA (UK)

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

BIG QUESTIONS What is technology's current emerging role in international diplomacy? Predictions and trade-offs

---

Engaging the audience with some of the big questions challenging leaders today.

1. What responsibility does the Chief Information Security Officer have in driving Innovation?
2. Should technology be a strategic concern within international diplomacy?
3. Cyber sanctions - Do institutions have the political will to act? How long will it take to build consensus and until it is applied to a nation state sponsor?
4. How can we manage in a world plagued by disinformation?

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Unique Keynote Cyber resilience for the aviation sector to enhance overall cyber preparedness

---

Dvir Rubinshtein

Aviation Security Operation Center Manager & Aviation Security Expert, Security Division (Israel)

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Keynote Understanding the criminal mind – how Western European BEC syndicates leverage business intelligence

James Linton,
Email Prankster – Threat Researcher, Agari

PULSE CONFERENCES

James Linton

Threat Researcher

@sinon_reborn

Agari Cyber Intelligence Division (ACID)

AGARI

An email prankster is hitting the CEOs of the world's biggest banks

Anjuli Davies and **Olivia Oran, Reuters**

Jun. 12, 2017, 5:06 PM 309

(Reuters) - The bosses of Wall Street banks Goldman Sachs and Citigroup are the latest executives to fall victim to an email prankster who has also managed to connect

SLATE

future tense ASU | NEW AMERICA | SLATE

That Email "Prank" Illustrates the Horrific Digital Security at Trump's White House

CNN politics

White House officials tricked by email prankster

FINANCIAL TIMES

Barclays' Staley and the foxhole prankster

The Telegraph

Business

WIRED

Hacking

Revealed: The real identity of prankster king SINON_REBORN

The man whose prank emails fooled Amber Rudd, Steve Bannon and Anthony Scaramucci reveals his true identity for the first time

FORTUNE

Even Goldman Sachs' CEO Is Falling for This Tricky Email Scam

An email prankster is hitting the CEOs of the world's biggest banks

Anjuli Davies and Olivia Oran, Reuters

Jun. 12, 2017, 5:06 PM

(Reuters) - The bosses of Wall Street banks Goldman Sachs and Citigroup are the latest executives to fall victim to an email prankster who has also managed to connect with the head of Barclays and the governor of the Bank of England.

Warner Bros.

TIME

White House Officials Were Duped by an 'Email Prankster,' Report Says

Search | Video | Rewards | Subscribe - 30 days free | Login | Register

The Telegraph HOME | NEWS | SPORT | BUSINESS | ALL SECTIONS

Business

Economy | Companies | Opinion | Open economy | Markets | Alex | More

Business

Bank of England Governor tricked by email prankster who conned Barclays boss Jes Staley

share

Save 9

SECTIONS | SEARCH | NEW YORK POST | TIPS

NEWS

Jared Kushner's lawyer tricked by email prankster twice in one week

By Bob Fredericks

September 28, 2017 | 10:06pm | Updated

TRENDING NOW ON NYPOST.COM

Girl catches deadly infection tryin on shoes while barefoot

VERDICT 3NCRYPT

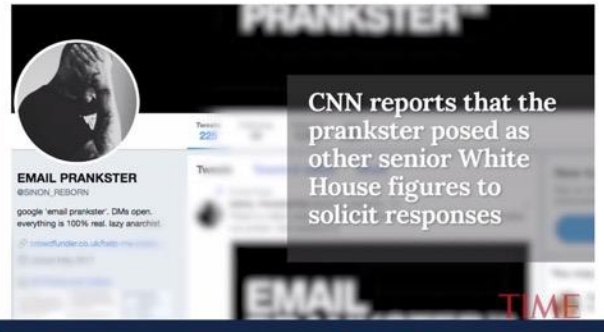
SHARE

IN THE NEWS

From the Email Prankster with Love

If the exploits of a man who calls himself the email prankster have taught us anything, it's that many high-profile figures aren't taking cybersecurity as seriously as they should. **Daniel**

Email Prankster, Report Says



Stories From

MERRIMENT

HOW TO PRANK THE RICH AND POWERFUL WITHOUT REALLY TRYING

The so-called "Email Prankster" has fooled the likes of Eric Trump and Anthony Scaramucci.

News | Policy | Opinion | Events | Jobs | HILL.TV

TRENDING: DONALD TRUMP JOHN MCCAIN FEATURED: RISING

Email prankster who tricked Eric

Tom Bossert

From Wikipedia, the free encyclopedia

Thomas P. Bossert (born March 25, 1975)[1] is an American lawyer and former Homeland Security Advisor to U.S. President Donald Trump.[2] He is currently an ABC News Homeland Security analyst.

Immediately before, he was a fellow at the Atlantic Council and prior to that he served as Deputy Homeland Security Advisor to President George W. Bush. In that capacity, he co-authored the 2007 National Strategy for Homeland Security. Prior to that, Bossert held positions in the Federal Emergency Management Agency, the Small Business Administration, the Office of the Independent Counsel, and the House of Representatives.[3] He also was appointed as the Director of Infrastructure Protection under Bush, overseeing the security of critical U.S. infrastructure, a post he held for two years.[4]

Bossert was appointed the Senior Director for Preparedness Policy within the Executive Office of the President.[5]

Contents [hide]

Early life and education [edit]

Bossert was born and raised in Quakertown, Pennsylvania,[6] where he graduated from Quakertown Community High School in 1993.[7] He attended the University of Pittsburgh, where he earned a Bachelor of Arts in Political Science and Economics in 1997, and attended George Washington University Law School, earning his Juris Doctor in 2003.[8]

Political career [edit]

Following the end of the Bush administration, Bossert was made a Nonresident Zurich Cyber Risk Fellow at the Atlantic Council's Cyber Security Initiative, a position he held until 2016. He also became president

Tom Bossert

7th United States Homeland Security Advisor

In office
January 20, 2017 – April 10, 2018

President	Donald Trump
Preceded by	Lisa Monaco
Succeeded by	Doug Fears

Personal details

Born	March 25, 1975 (age 44) Quakertown, Pennsylvania, U.S.
Political party	Republican
Education	University of Pittsburgh (BA) George Washington University (JD)

Tom Bossert

From Wikipedia, the free encyclopedia

Thomas P. Bossert (born March 25, 1975)[1] is an American lawyer and former Homeland Security Advisor to U.S. President Donald Trump.[2] He is currently an ABC News Homeland Security analyst.

Immediately before, he was a fellow at the Atlantic Council and prior to that he served as Deputy Homeland Security Advisor to President George W. Bush. In that capacity, he co-authored the 2007 National Strategy for Homeland Security. Prior to that, Bossert held positions in the Federal Emergency Management Agency, the Small Business Administration, the Office of the Independent Counsel, and the House of Representatives.[3] He also was appointed as the Director of Infrastructure Protection under Bush, overseeing the security of critical U.S. infrastructure, a post he held for two years.[4]

Bossert was appointed the Senior Director for Preparedness Policy within the Executive Office of the

Tom Bossert

In July 2017, a British hacker spear-phished Bossert into thinking he was Jared Kushner by sending an email to Bossert. The hacker also received Bossert's private email address without asking for it.[10]

7th United States Homeland Security Advisor	
In office	January 20, 2017 – April 10, 2018
President	Donald Trump
Preceded by	Lisa Monaco
Succeeded by	Doug Fears
Personal details	
Born	March 25, 1975 (age 44) Quakertown, Pennsylvania, U.S.
Political party	Republican
Education	University of Pittsburgh (BA) George Washington University (JD)

Early life and education [edit]

Bossert was born and raised in Quakertown, Pennsylvania,[6] where he graduated from Quakertown Community High School in 1993.[7] He attended the University of Pittsburgh, where he earned a Bachelor of Arts in Political Science and Economics in 1997, and attended George Washington University Law School, earning his Juris Doctor in 2003.[8]

Political career [edit]

Following the end of the Bush administration, Bossert was made a Nonresident Zurich Cyber Risk Fellow at the Atlantic Council's Cyber Security Initiative, a position he held until 2016. He also became president

From	**Jared Kushner** < outlook.com >
To	**Tom P. Bossert EOP/WHO** < White House >
Subject	**August 26th**

Tom, we are arranging a bit of a soirée towards the end of August. It would be great if you could make it, I promise food of at least comparible quality to that which we ate in Iraq!

Should be a great evening.

Jared

From	**Jared Kushner** < outlook.com >
To	**Tom P. Bossert EOP/WHO** < White House >
Subject	**August 26th**

Tom, we are arranging a bit of a soirée towards the end of August. It would be great if you could make it, I promise food of at least comparible quality to that which we ate in Iraq!

Should be a great evening.

Jared

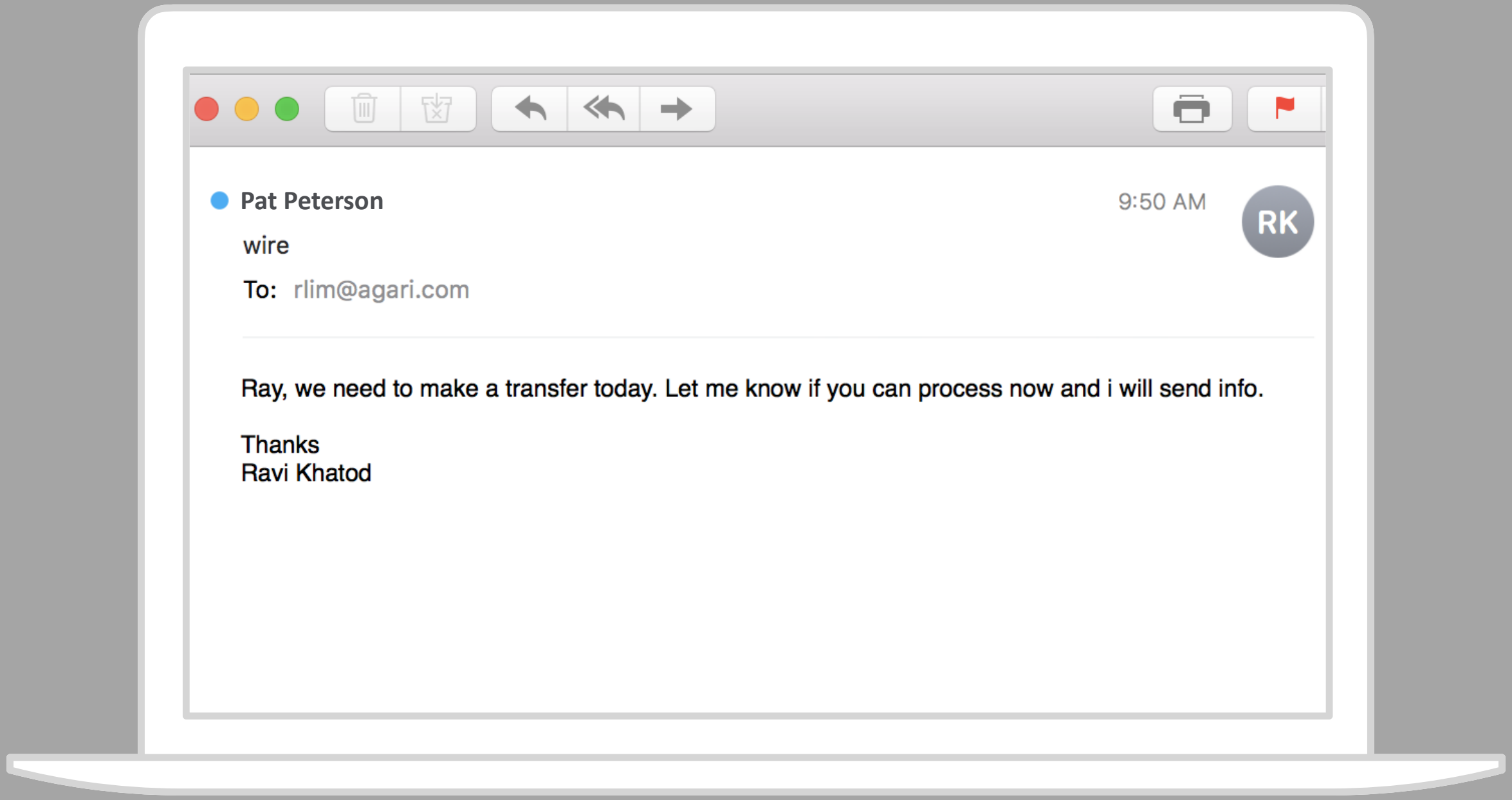
From	**Tom P. Bossert EOP/WHO** < White House >
To	**Jared Kushner** < outlook.com >

Thanks, Jared.

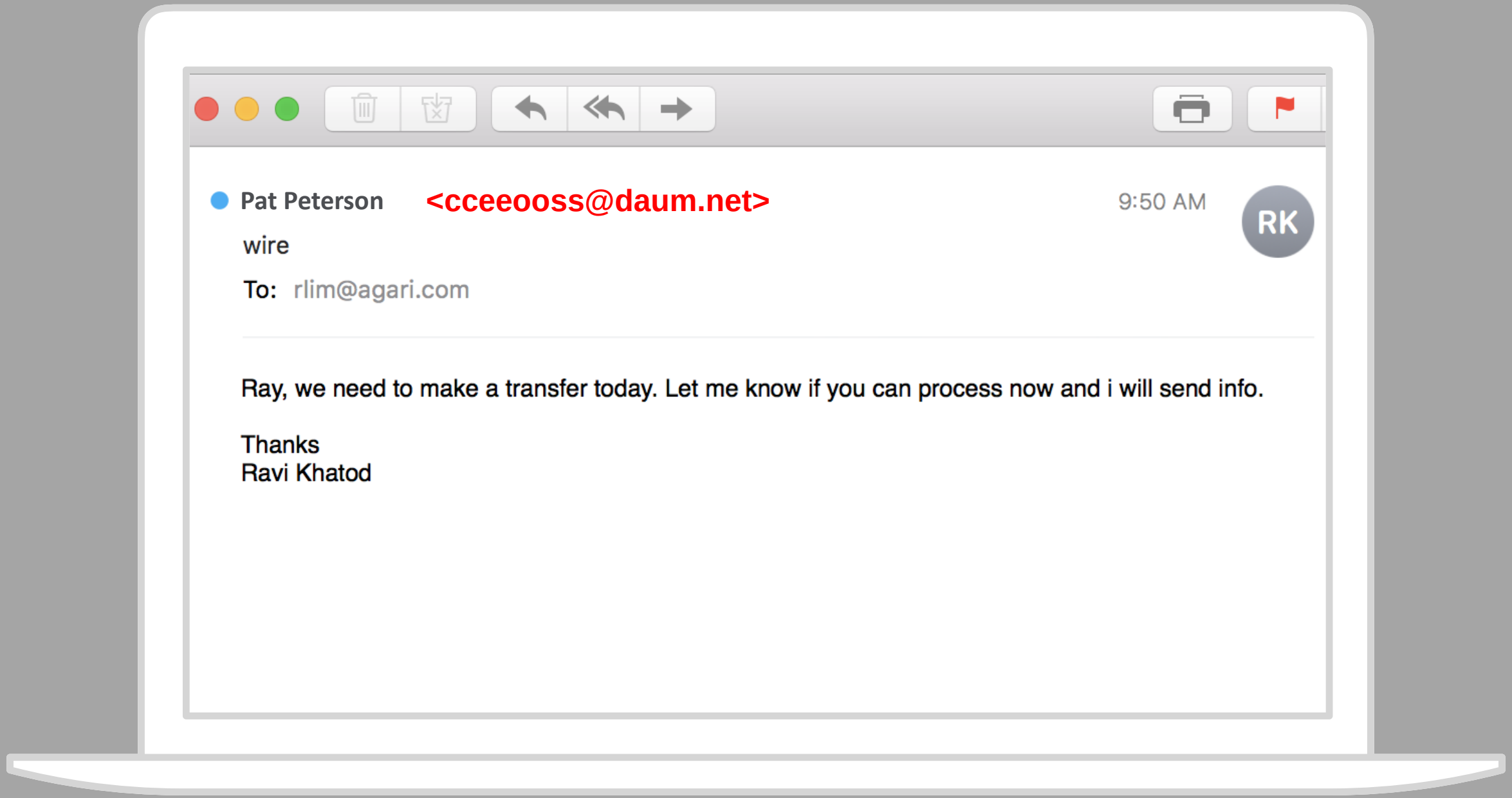
With a promise like that, I can't refuse.
Also, if you ever need it, my personal email is [**Redacted**]

-Tom

What can we learn from this?


Pat Peterson
9:50 AM
RK
wire
To: rlim@agari.com
Ray, we need to make a transfer today. Let me know if you can process now and i will send info.
Thanks
Ravi Khatod

AGARI


Pat Peterson
<cceeooss@daum.net>
9:50 AM
RK
wire
To: rlim@agari.com
Ray, we need to make a transfer today. Let me know if you can process now and i will send info.
Thanks
Ravi Khatod

AGARI

Active Engagement

Attacker

ACID
AGARI CYBER
INTELLIGENCE DIVISION

ACID (us!)

Victim

AGARI

Active Engagement

Attacker

ACID

AGARI CYBER
INTELLIGENCE DIVISION

Victim

AGARI

Active Engagement

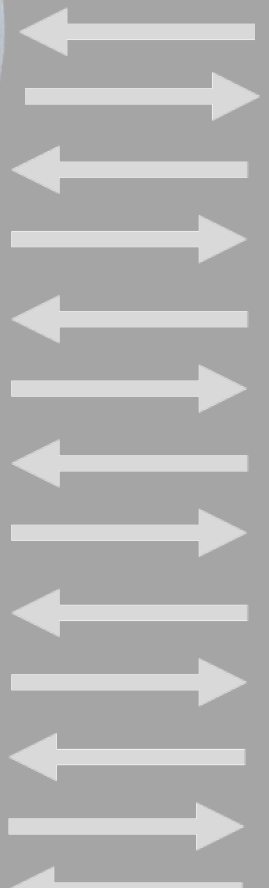
Attacker

ACID
AGARI CYBER
INTELLIGENCE DIVISION

Victim

Active Engagement

Attacker



ACID

Victim

AGARI

Why Engage?

Geolocational data

Tactics & Techniques

Mule Accounts

Social Media

Attacker

Use

Intel for Law Enforcement

Track Trends & Evolutions

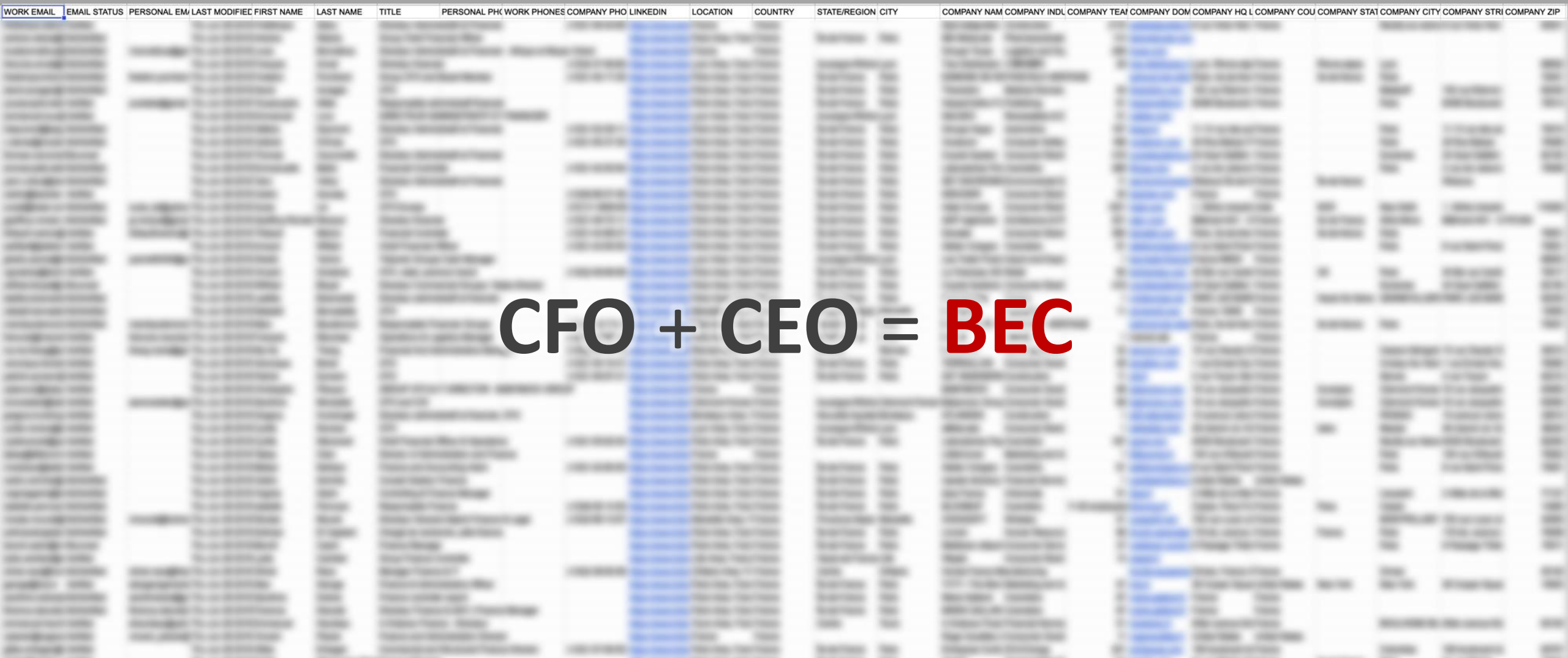
Report to Banks

Attribution

AGARI

Cyber-Criminals use Mainstream Business Intelligence

Cyber-Criminals use Mainstream Business Intelligence



3rd CISO 360 CONGRESS 2019 Rome

Panel Cyber Crime - How are AI/ML and disruptive technologies supporting sustainable, ethical and forward-thinking operations?

Chaired by:

Dr. Vasileios Karagiannopoulos, Senior Lecturer in Law and Cybercrime, Institute of Criminal Justice Studies, University of Portsmouth (UK)

Panellists:

Friedelien Brockerhoff, GM: Group Information Security Program, MTN (South Africa)

Mariana Pereira, Director, Darktrace

Tom Gamali, Group CISO & Global Head of Business Resilience, Abdul Latif Jameel, Company (Kuwait)

James Linton, (Email Prankster!) Threat Researcher, Agari

Dave Tyrrell, SailPoint

Ben Jeffreys, Senior Executive, Nominet

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

LEAD QUESTIONS: Panel Cyber Crime - How are AI/ML and disruptive technologies supporting sustainable, ethical and forward-thinking operations?

- Defining the current state of ML and AI technologies
- Ethical dimensions and practical challenges of developing and implementing ML/AI applications and other advanced technologies such as facial recognition
- Protecting businesses and organisations against harmful practices and cyber enabled crime • Adversarial ML intelligence – is this being used currently to develop and challenge ML/AI systems in cybersecurity and how?
- How do these technologies align with the potentially conflicting interests and aims of law enforcement, businesses and governments?

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Keynote 10 proven ways in 10 minutes to develop a GDPR-ready incident and breach 72-hour action plan!

Vipul Asher
Privacy Consulting Manager, OneTrust

PULSE CONFERENCES

Developing a GDPR-Ready Incident & Breach 72-Hour Action Plan

Vipul Asher - CIPP/E

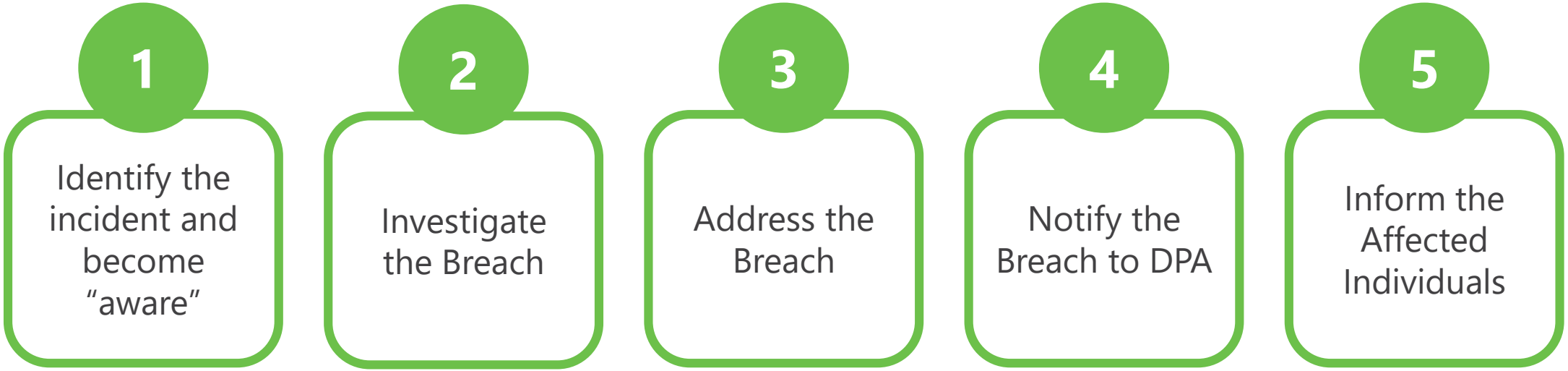
OneTrust
Privacy Management Software

Prior to a Breach

1. Up-to-date Data Mapping
2. Vendor Management
3. Tech & Org. Security Measures
4. Written Privacy & Risk Policies
5. Internal Trainings
6. Reporting Mechanism
7. Notification Obligations
8. Breach Documentation

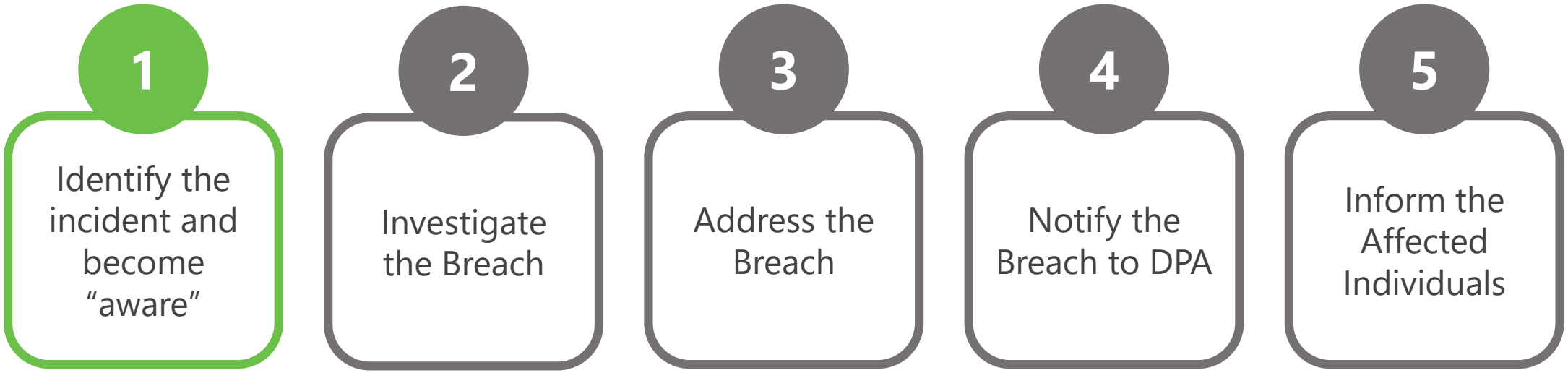
OneTrust
Privacy Management Software

72-Hour Action Plan



Not all incidents proceed into all of the stages above. This is the maximum.

Identify the incident and become aware



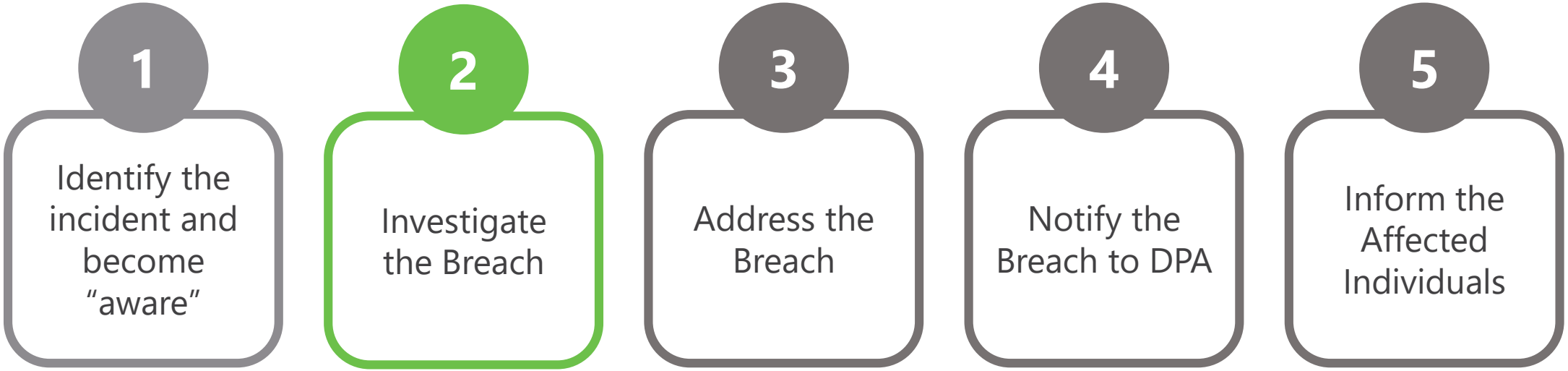
When does the clock start ticking?

When does controller become aware?

- EDPB (WP29): When the controller has a **reasonable degree of certainty** that a security incident has occurred that has led to **personal data being compromised**.

Incident	Aware when
A USB with encrypted personal data was lost, and it is not possible to ascertain whether unauthorized persons gained access.	The controller realized the USB key had been lost.

Investigate the Breach

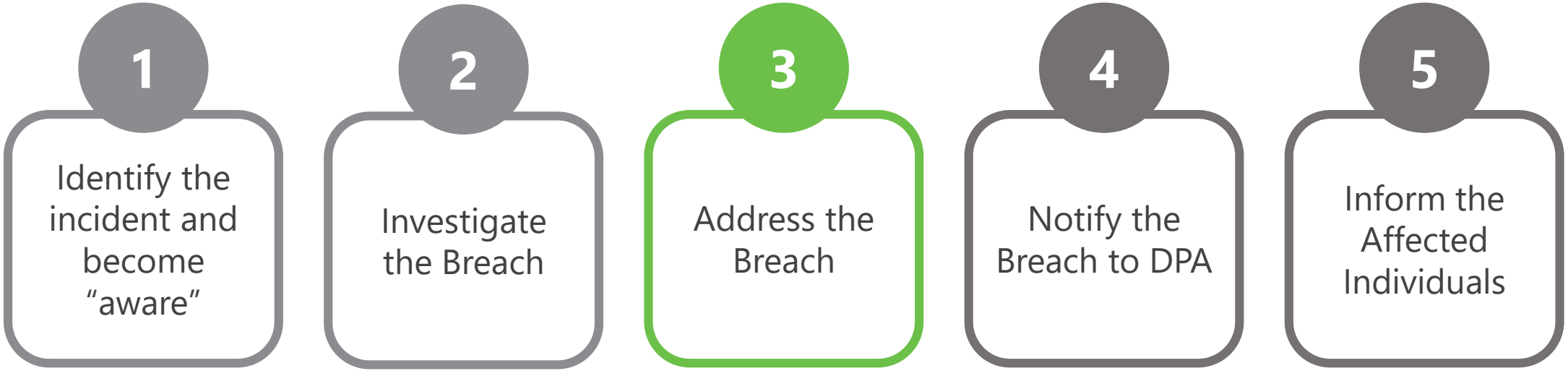


Most of the 72 hours should be spent on this step

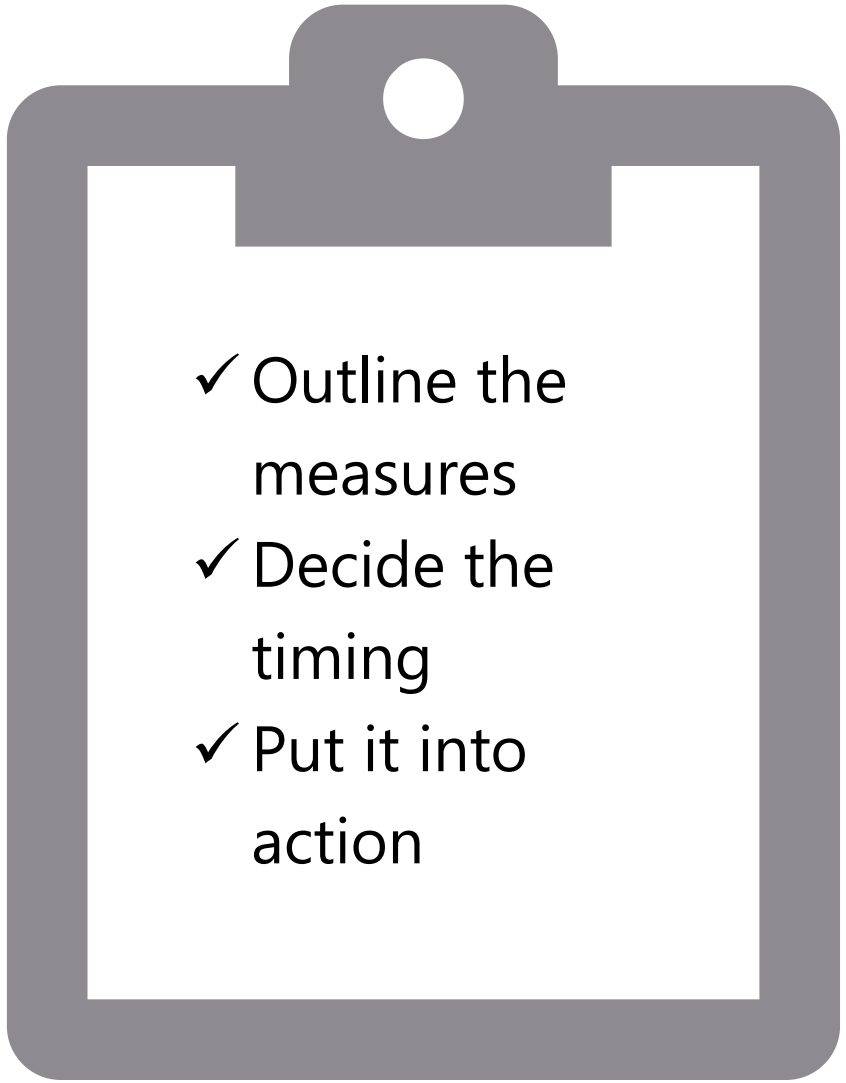
What is a “Personal Data Breach”?

Personal Data Breach	a breach of security leading to the **accidental or unlawful** destruction, loss, alteration, unauthorized disclosure of, or access to, **personal data** transmitted, stored or otherwise processed.”
Confidentiality Breach	disclosure of, or access to, personal information
Integrity Breach	alteration of personal data
Availability Breach	loss of access to or destruction of personal data
Less Obvious Examples	e-mail is sent to a wrong person, old ICT equipment was disposed of without erasing the data, lost phone, power outage affecting the company’s access to data

Address the Breach

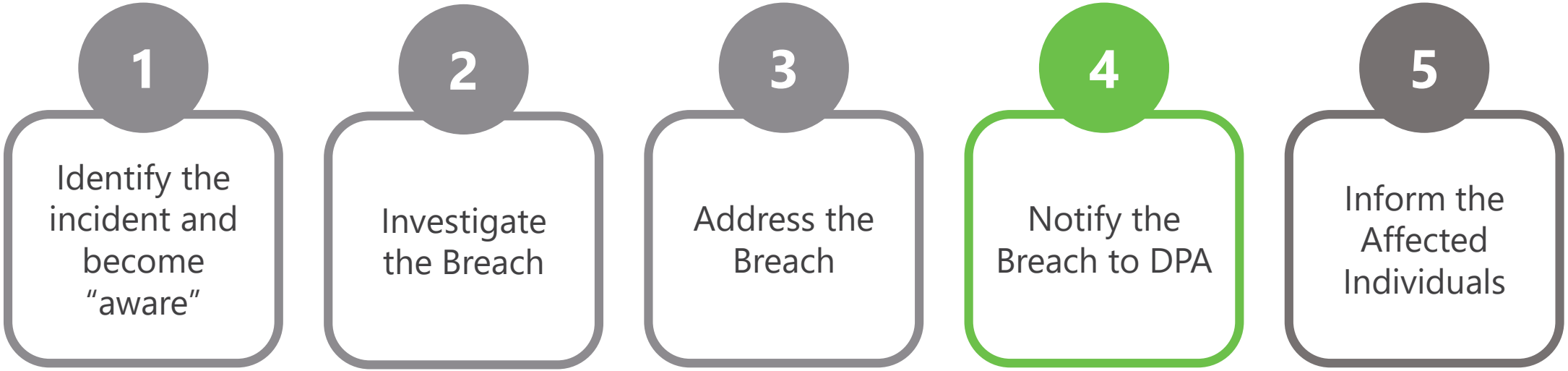


Make your Breach Response Plan



- There is **no one-size-fits-all**, every breach is unique and requires different approach.
- Focus of any breach response plan should be on **protecting individuals** and their personal data
- Evaluate **all possible consequences** of the breach – Security team should work very closely on this with Privacy Team.
- Make sure to have thorough **breach detection and analysis process** in place to identify all consequences of a breach.

Notify Data Protection Authorities (DPAs)



Notify Data Protection Authorities (DPAs)

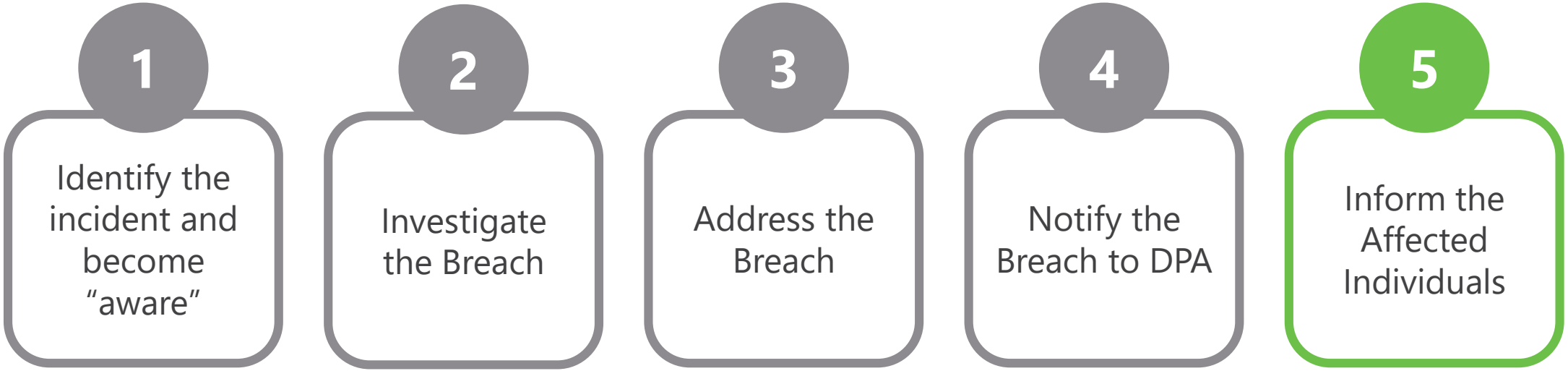
Assessment on DPA jurisdiction – choosing which DPA to notify

- Consider whether the breach impacted a cross-border processing (occurred outside the EU, various EU Member State residents affected). One-Stop-Shop is not always applicable.
- DPO or senior Privacy team member can be helpful at this stage.

Breach Notification – Initial or Complete Notification?

- Include an assessment whether the organization prefers to make a complete notification straight away, or
- Prefers to submit an initial notification which is then followed by further information, once obtained
- Further communication with the DPA, submitting of documents etc.

Tell the Individuals



Information to Individuals

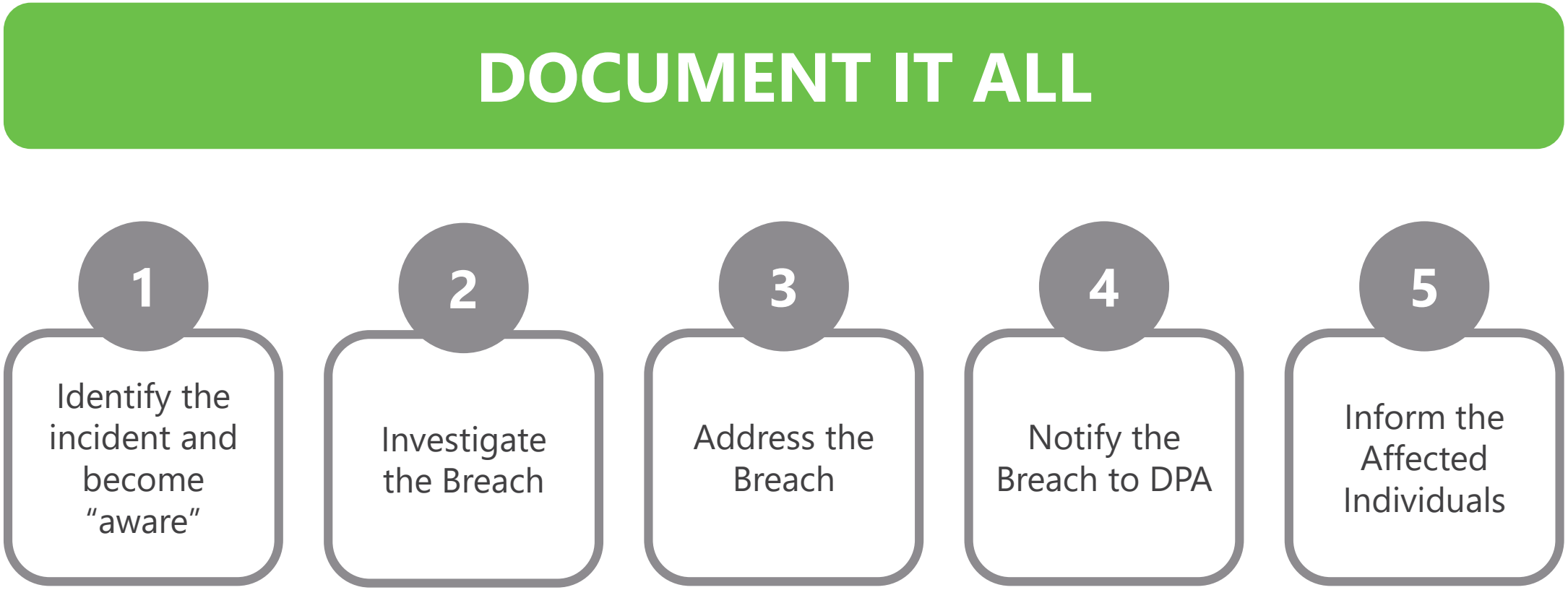
Do we tell them?

- Risk assessment is KEY again – focal point: likely high risk to the rights and freedoms of the individuals.
    - = higher risk threshold than for notifying DPAs
- Important point – wrong assessment of risks associated with a particular data breach = risk of high penalties for not reporting. As a result, we see a lot of over-reporting these days.

What do we tell them?

- Good measure – some portions of the information can be pre-drafted to save time
- GDPR Art. 34(2): minimum content –
    - a description of the nature of the breach;
    - the name and contact details of the data protection officer or other contact point;
    - a description of the likely consequences of the breach; and
    - a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Document it All



OneTrust Privacy Management Software Platform

Privacy Program Management

Maturity & Benchmarking
Executive Scorecard

DataGuidance Research
In-Depth Legal Portal

Assessment Automation
PIA | DPIA | PbD | InfoSec

Data Mapping
Discovery | ROPA | Inventory

Targeted Data Discovery
Access | Deletion | Portability

Privacy & Marketing User Experience

Cookie Compliance
Powered by Cookiepedia™

Mobile App Compliance
Scanning & Consent

Consent & Preferences
Universal Preference Center

Data Subject Rights
From Intake to Fulfillment

Policy & Notice
Centrally Host, Track & Update

Vendor Risk Management

Vendor Assessments
Security & Privacy Risk

Vendorpedia™ Exchange
Third-Party Risk Exchange

Contracts & DPAs
Legal Document Integration

Ongoing Monitoring
Privacy & Security Threats

Chasing Services
Managed Services

Incident and Breach Response

Incident Intake
Centralized Register

DataBreachpedia™
300+ Indexed Breach Laws

Risk Assessments
Risk and Harms Analysis

Notification & Reporting
Obligation Tracking

Real-Time Activity Feed
Breaches & Enforcements

OneTrust
Privacy Management Software

OneTrust

Privacy Management Software

Visit Our Stand

Product Demos

Full Text GDPR Books

Free Tools & Templates

GDPR Workshops

OneTrust
Privacy Management Software

PrivacyConnect

CCPA & GDPR Community by OneTrust

250+ Events Across 100+ Global Cities

Free CCPA & GDPR Workshops

5 CPE Credit Hours

OneTrust Certification Program in Select Cities

Monthly Privacy Webinar Series

Hosted by Top Tier Law Firms & Consultancies

Local Community Chapters

Latest Privacy News & Events in your City

Amsterdam	Rome	San Francisco	Philadelphia
Dublin	Brussels	Chicago	Minneapolis
London	Prague	New York	Detroit
Paris	Manchester	Washington DC	Portland
Oslo	Tel Aviv	Atlanta	Kansas City
Stockholm	Lisbon	Houston	Raleigh
Helsinki	Budapest	Toronto	St. Louis
Belfast	Stuttgart	Denver	San Diego
Geneva	Berlin	Phoenix	Austin
Zurich	Bucharest	Boston	Cleveland
Warsaw	Barcelona	Charlotte	Hong Kong
Vienna	Frankfurt	Seattle	Sydney
Milan	Dubai	Columbus	Melbourne
Madrid	Doha	Los Angeles	Singapore
Athens	Abu Dhabi	Indianapolis	Seoul

”This was the best GDPR-focused conference I have ever been to. This was not just a high-level look into requirements, but an in-depth educational experience for myself and my colleagues.”

VIEW FULL SCHEDULE

PrivacyConnect.com

OneTrust
Privacy Management Software

Questions?

OneTrust
Privacy Management Software

3rd CISO 360 CONGRESS 2019 Rome

Innovation Insights Quantum-a double-edged sword? How do we future Quantum-proof our current and future infrastructures?

Led by: Dr. Eduardo Solana, Senior Lecturer of Cryptography and Security, University of Geneva
Olivier Pfeiffer, Head of Finance and Critical Infrastructure Markets, ID Quantique (Switzerland)

PULSE CONFERENCES

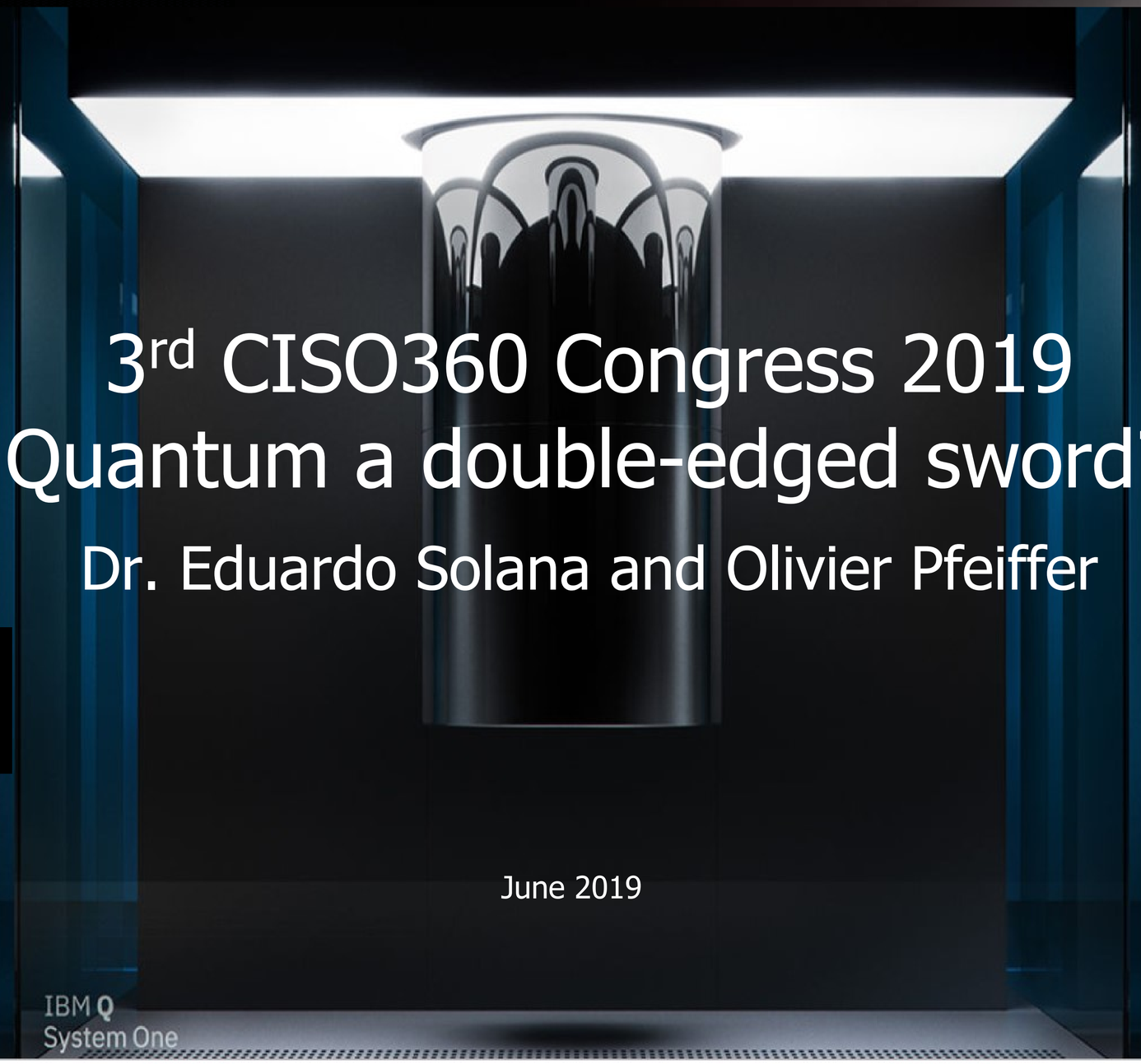
3rd CISO360 Congress 2019
Quantum a double-edged sword?

Dr. Eduardo Solana and Olivier Pfeiffer

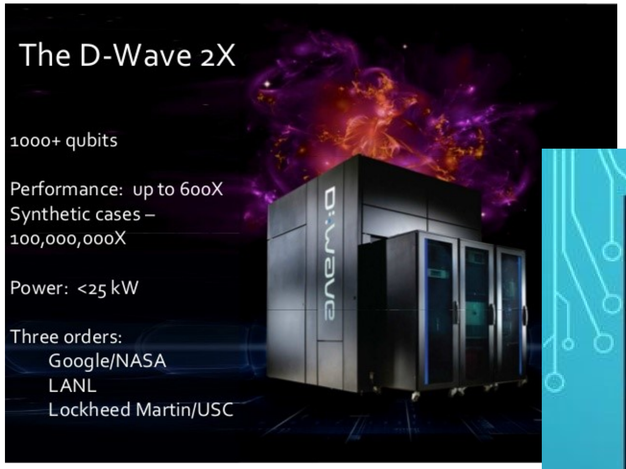
UNIVERSITÉ DE GENÈVE

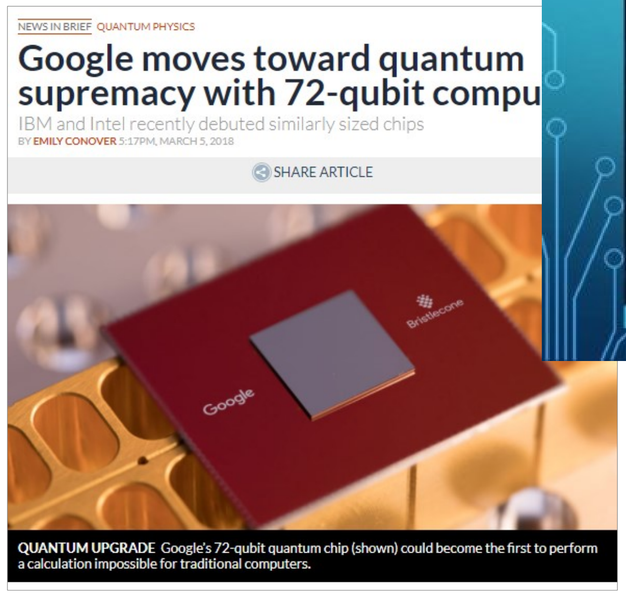
IDQ

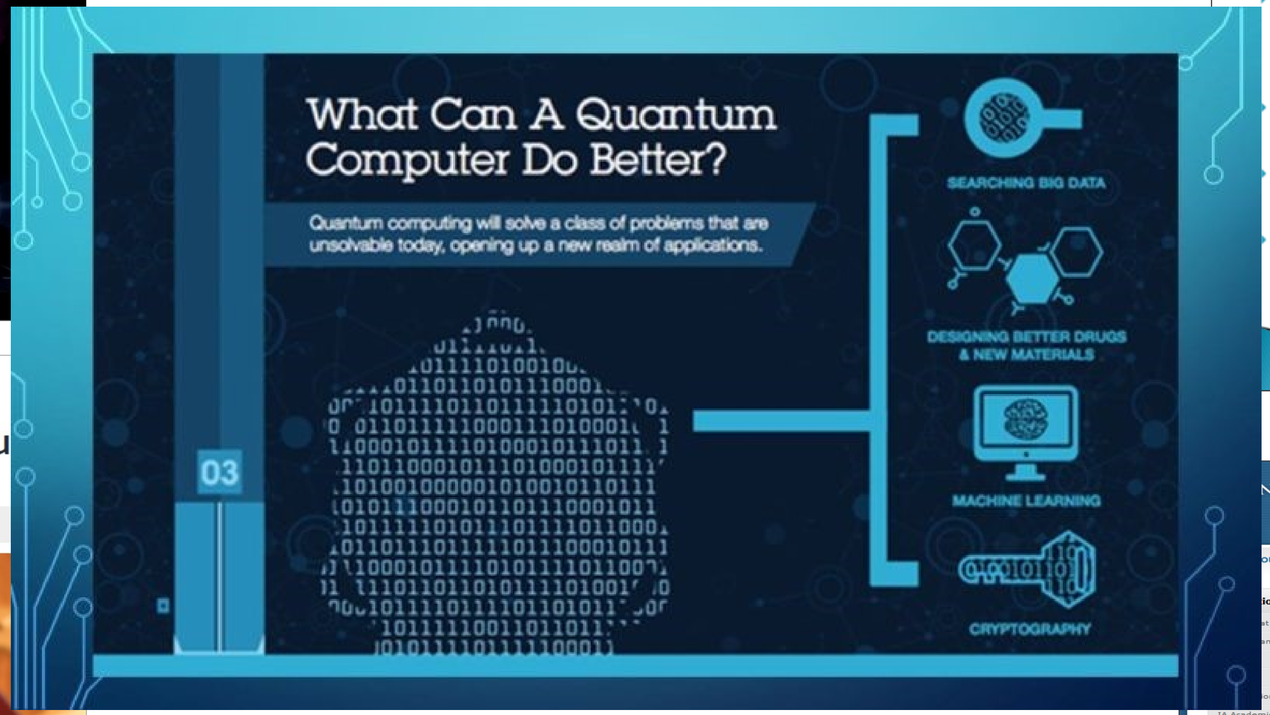
June 2019

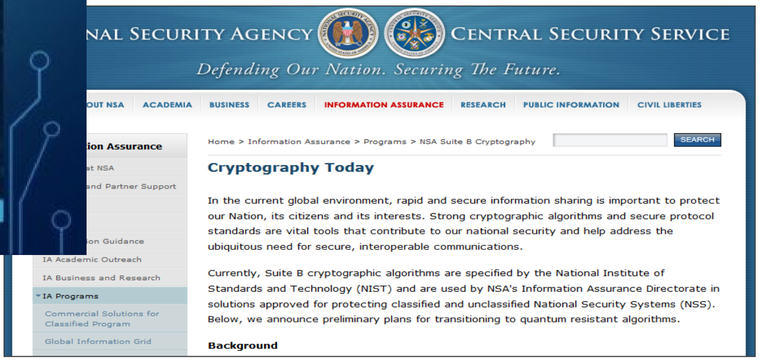


Quantum computing is here!









"We announce preliminary plans for transitioning to quantum resistant algorithms to provide security against a potential quantum computer" - Aug. 2015

UNIVERSITÉ DE GENÈVE

IDQ

Quantum technology repercussion

Impact on current cryptography:

- Symmetric Algorithms: **Increase key sizes** (256 bits minimum) – Grover's theorem
- Crypto hashes and MACs: **Increase digests and MAC-values** (512 bits minimum) – Grover's theorem
- Asymmetric (public-key) Algorithms: **Totally broken** by Shor's theorem. This includes **most current encryption and signature schemes as well as key establishment protocols !**

In the Internet: Symmetric algorithm resistance is irrelevant since crypto keys are shared through quantum unsafe asymmetric primitives…

Internet cryptography totally devastated by the "quantum quake" !

On the positive side

- Quantum enables **best quality** (*maximum entropy*) **random key generation** strengthening current and future algorithms
- **Quantum key distribution** protect secrets from unauthorized disclosure (proven by quantum physics)
- **Mathematical problems intractable to date will become feasible** by a powerful and universal quantum computer: *factoring*, *discrete logarithms*, *finite fields computation*, optimization problems, etc.

Quantum computing will bring countless benefits to science and society (healthcare, physics, biology, finance, etc.)

UNIVERSITÉ DE GENÈVE

IDQ

When to prepare?

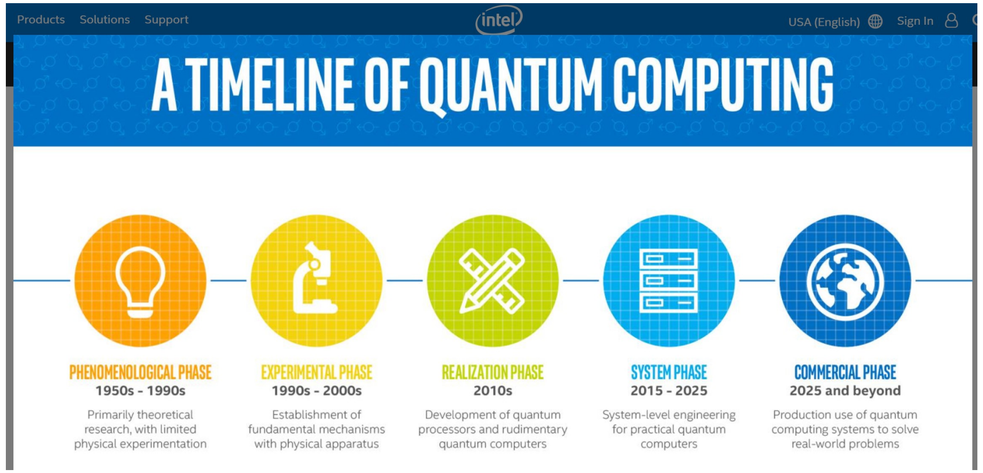
Large-scale quantum computing is 10-15 years away
1 in 7 chance of crypto primitives being affected by quantum attacks in 2026
1 in 2 chance by 2031

Estimates by Prof. Michele Mosca
Institute for Quantum Computing
University of Waterloo
(at ETSI/IQC workshop 09/2017)

NIST points out that we can make a strategic choice on when to worry about quantum computing by looking at three questions:

- How long does my encryption need to be secure (x years)?
- How long will it take to re-tool my existing infrastructure with a quantum-safe solution (y years)?
- How long will it be until a large-scale quantum computer is built (z years)?

- **If x + y > z for your company, then you should start making steps to prepare now.**



Screen capture from Intel's website:https://www.intel.com/content/www/us/en/research/quantum-computing.html

UNIVERSITÉ DE GENÈVE

IDQ

A recent call…

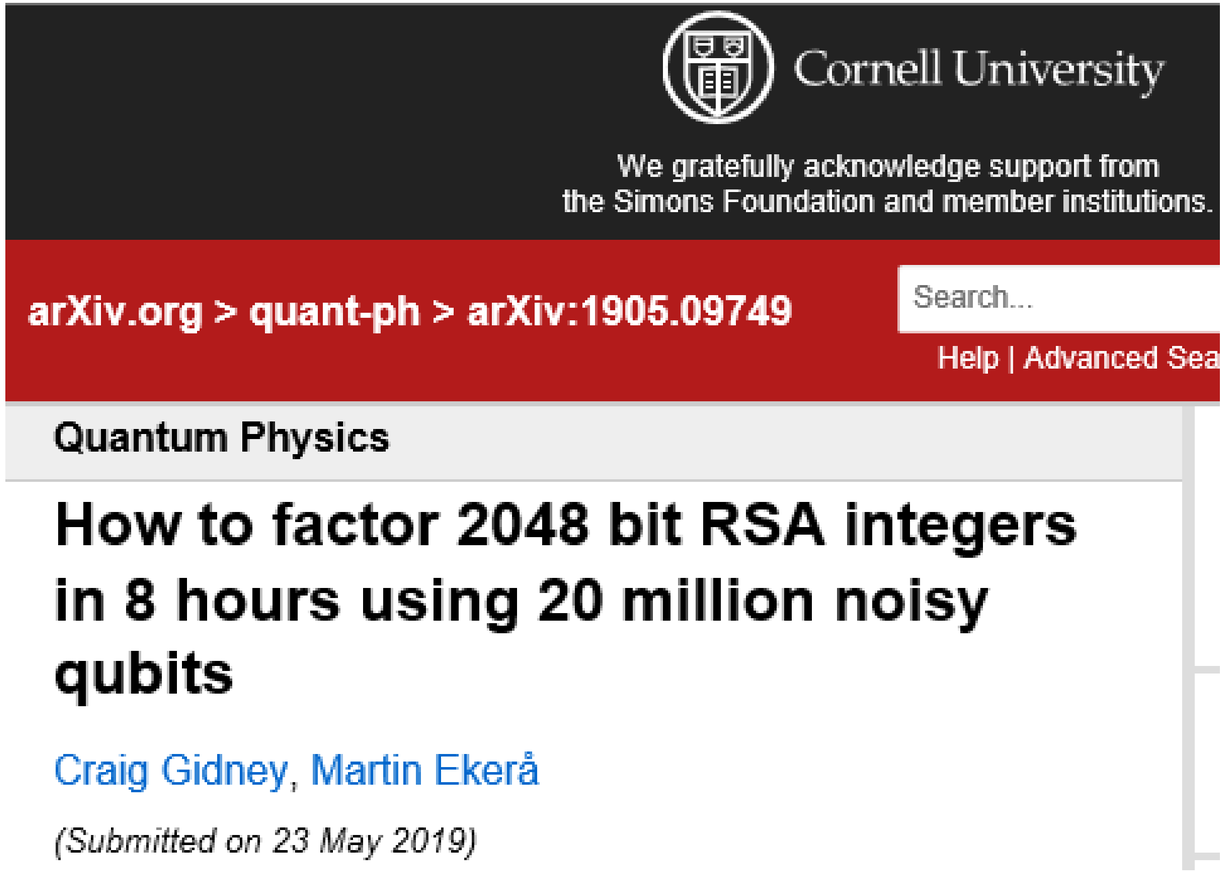
MIT Technology Review

Computing

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

by **Emerging Technology from the arXiv** May 30, 2019



UNIVERSITÉ DE GENÈVE

IDQ

Paving the way for the *quantum-safe cryptography* era

- **Post-Quantum Cryptography** (**PQC**) research rapidly gaining traction
- Multiple public-key cryptography quantum-safe alternatives explored:
  - *Lattice-based cryptography*
  - *Multivariate polynomials*
  - *Correcting codes-based algorithms*
  - *Hash-based cryptography for digital signatures, etc.*
- Interesting results achieved on these fronts but generalized consensus underlines the lack of maturity, in-depth evaluation and cryptanalysis resistance of current PQC candidates
- In 2016 **NIST** issued a Call for Proposals for PQC algorithms. First round features 82 initial candidate algorithms. As of today, 17 encryption/key establishment and 9 digital signature candidates remain in 2nd round. **Expected standard drafts not expected before 2022 – 2024**
- In August 2015 **NSA** released a surprising statement **on the need to transition to PQC algorithms** provoking reluctancy and generalized speculation in the crypto community…

Crypto-Agility transcends promising new technologies !

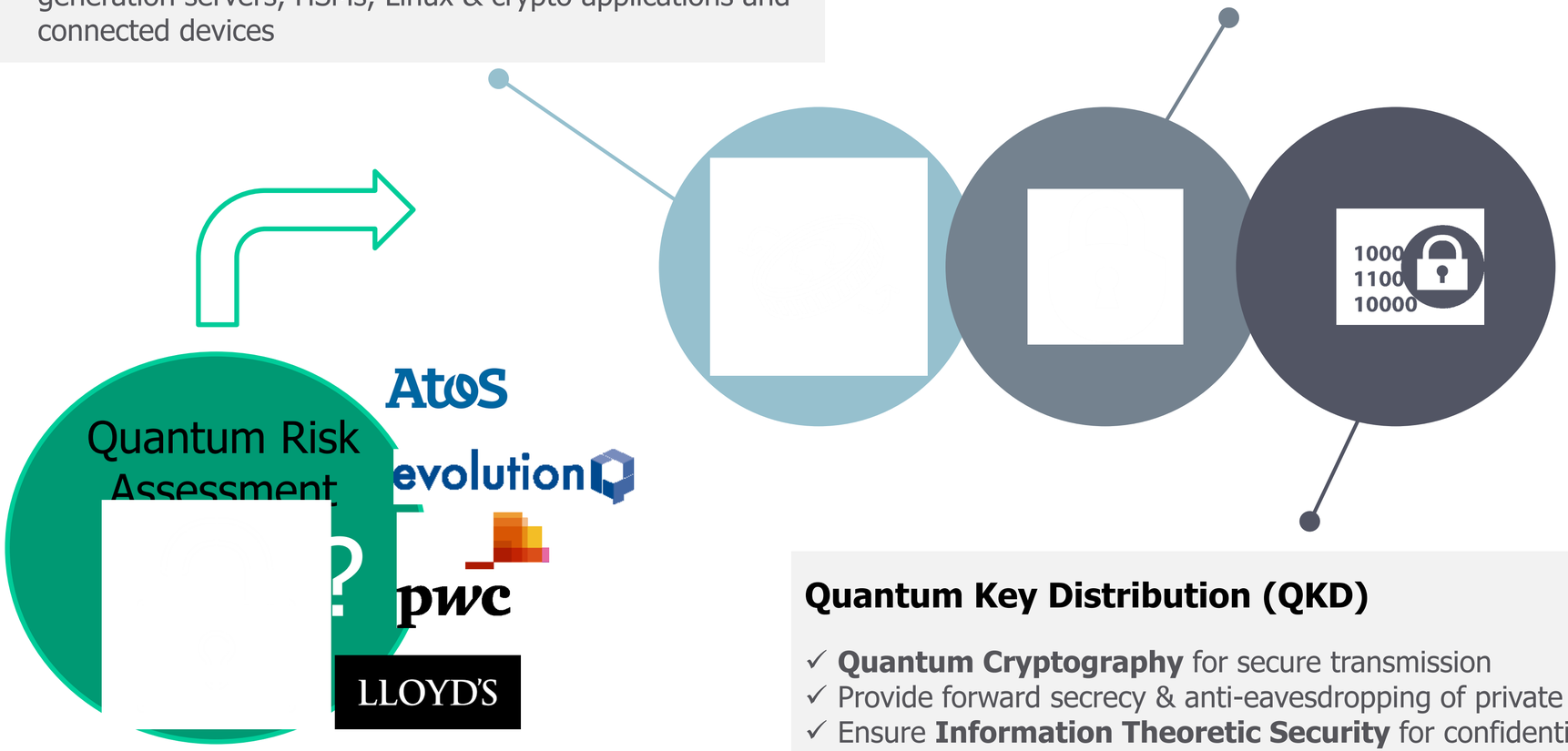
IDQ Recommended Path to Quantum Safety

Quantum Random Number Generation (QRNG)

- ✓ **Instantly strengthen your crypto key material**
- ✓ Feed higher quality (Swiss trusted) entropy into key generation servers, HSMs, Linux & crypto applications and connected devices

Crypto agility to move to Post Quantum Crypto

- ✓ Be **crypto-agile** to move to next generation Post Quantum Crypto
- ✓ Be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further



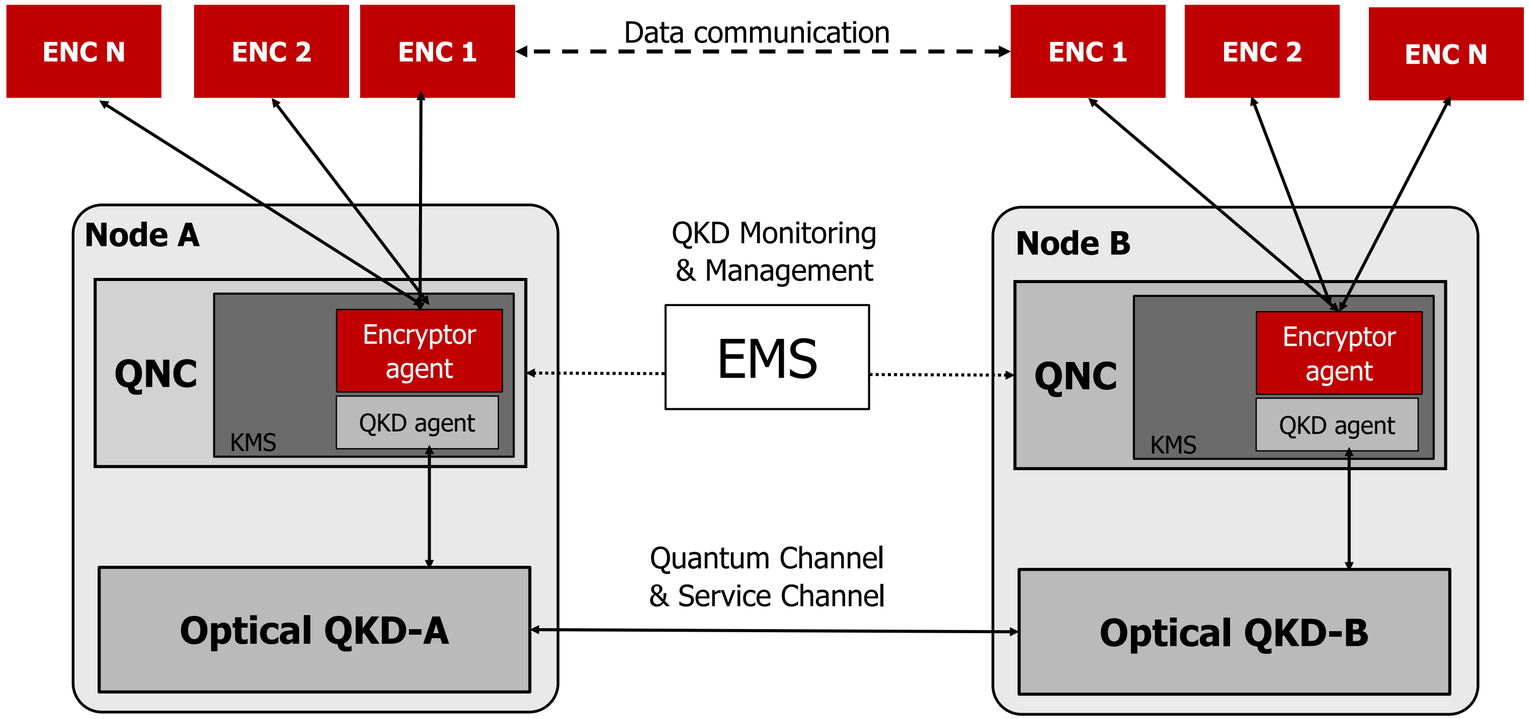
Quantum Key Distribution (QKD)

- ✓ **Quantum Cryptography** for secure transmission
- ✓ Provide forward secrecy & anti-eavesdropping of private key exchange/back up
- ✓ Ensure **Information Theoretic Security** for confidentiality to guarantee ownership for the next decade (Post-Quantum era)
- ✓ Use QKD today for backend **IP protection**

UNIVERSITÉ DE GENÈVE

IDQ

Typical Quantum Key Distribution & Encryption



Dedicated Network Encryption (L2)

SafeNet THALES

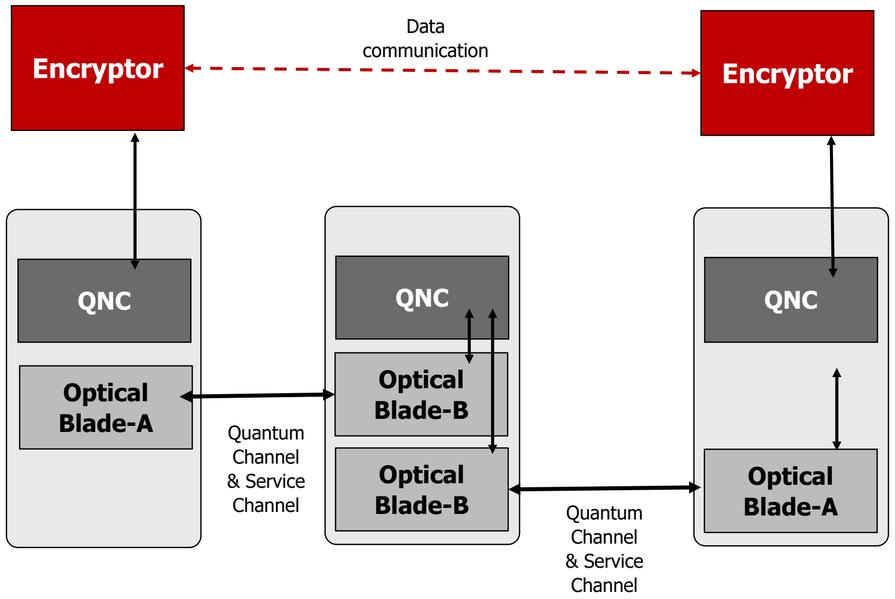
Optical Equipment Vendors (L1)

NOKIA ciena ADVA Optical Networking

Specialized Networking Vendors

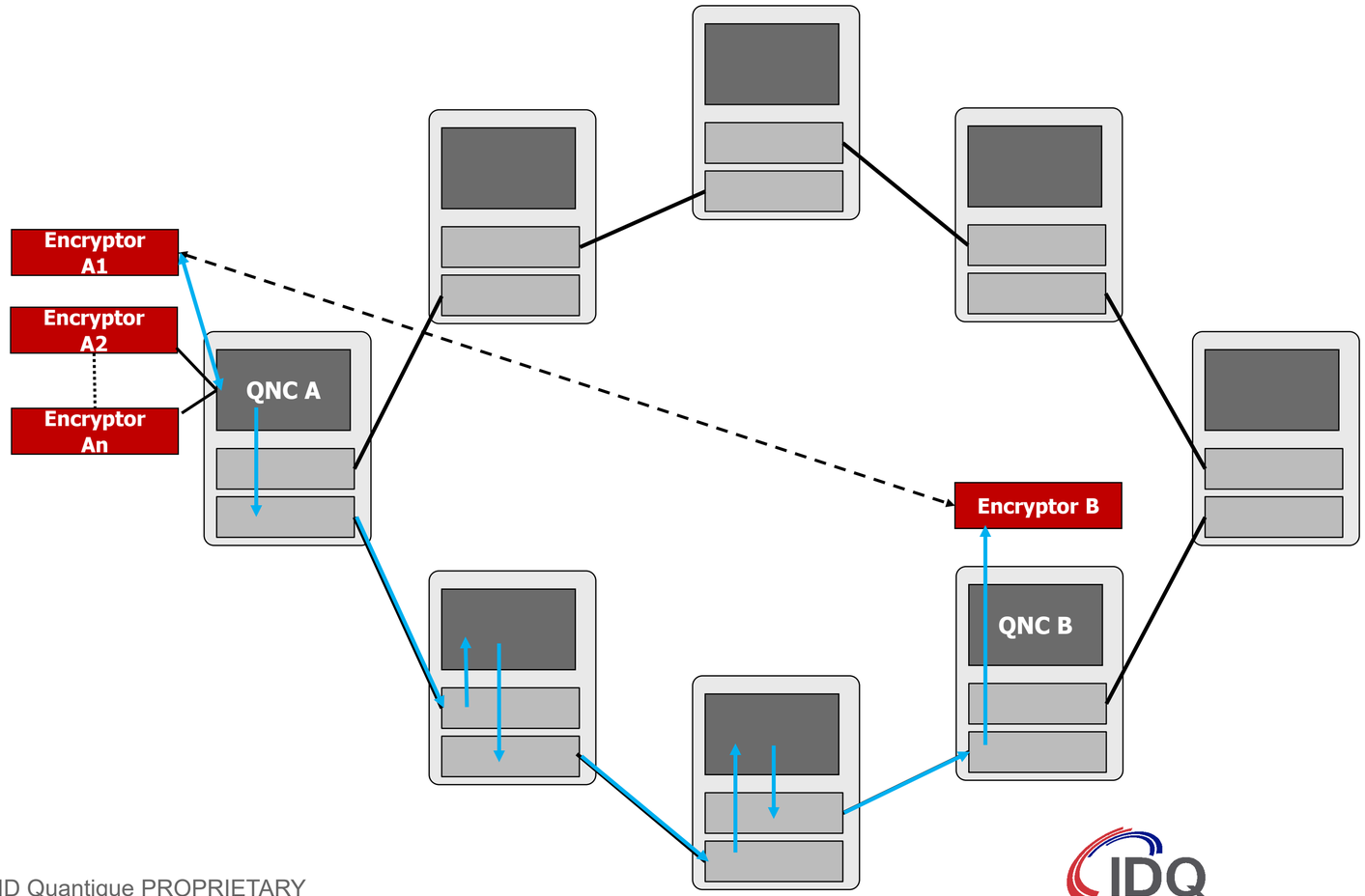
ABB

QKD Relay Nodes and Ring topology



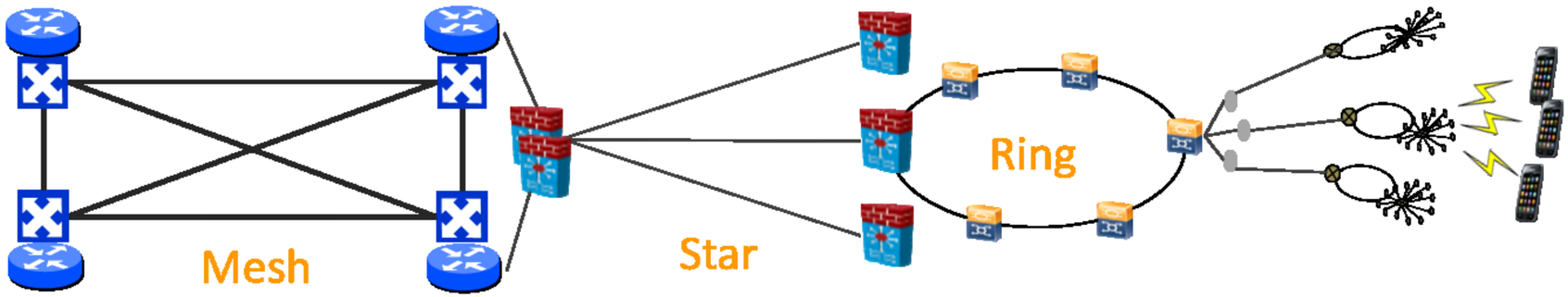
Forward function to distribute keys over long distances

Add/drop or forward in ring topology (up to 16 nodes)



Current Example: Quantum-Safe 5G

Backbone	Core	Access



SK telecom

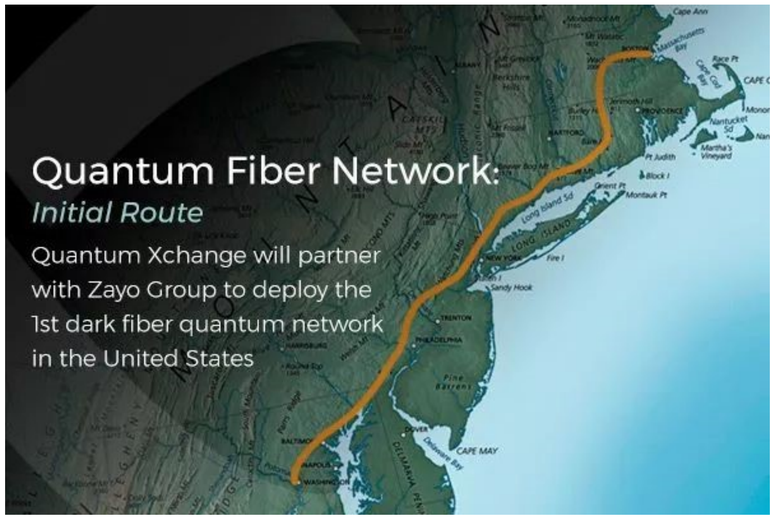
Quantum Key Distribution

5G standard security & QRNG

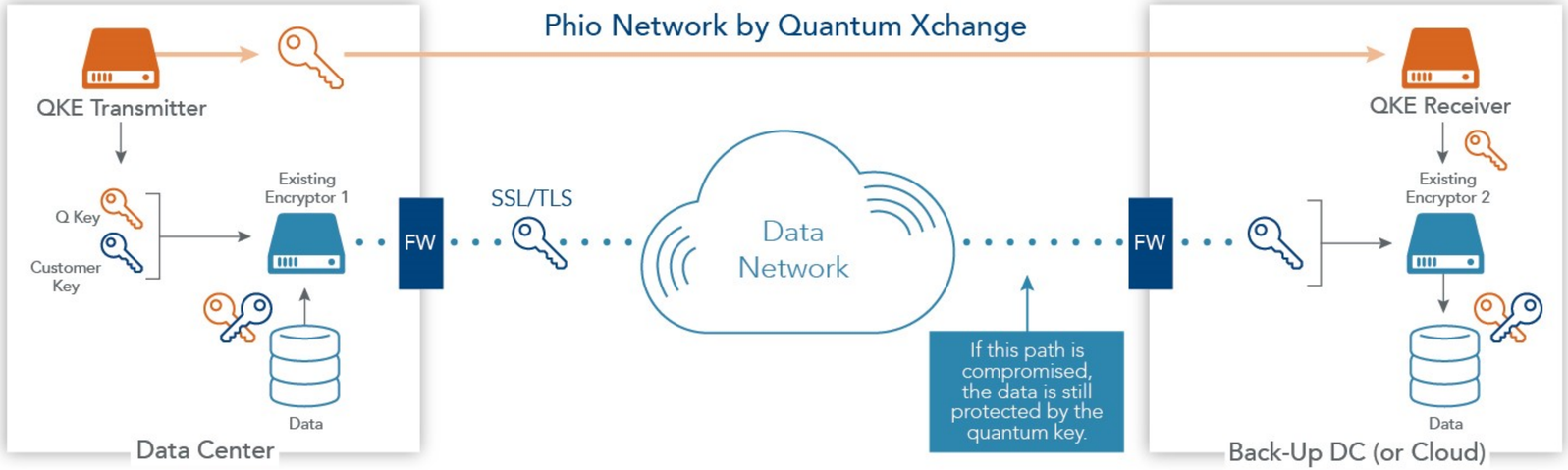
UNIVERSITÉ DE GENÈVE

IDQ

Current Example: Commercial QKD Networks (QKD as a Service)



QUANTUMXCHANGE



CAS Quantum Network

National Quantum Secure Communication Backbone Network (Phase I, 2018~2020)

Coverage area

Total Distance: ~ 11000 km

Backbone network: ~ 8000 km

City access network: ~ 3000 km

Main function

Serve for national strategy

Integration in Jing-Jin-Ji Area

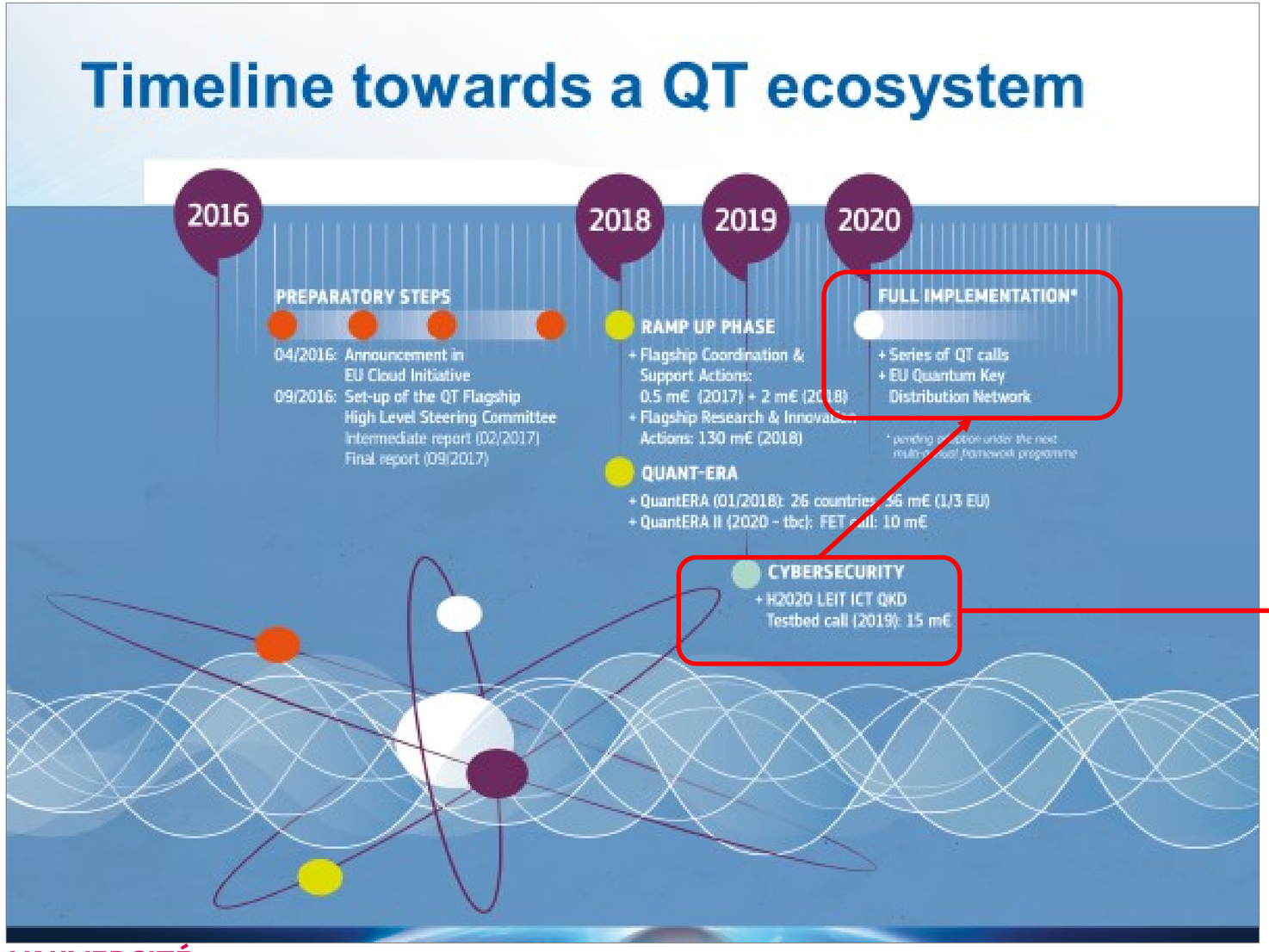
The Yangtze Economic Zone

The Belt and Road Initiative, and etc.

Serve for financial sectors and governments

Explorer applications in education and medical fields

QT Vision in Europe



«Quantum Flagship» (qt.eu)
1B€ for Quantum Technologies (2018-2027)

Testbed – 15M€ - 2019-2021

Standization Activities around QKD

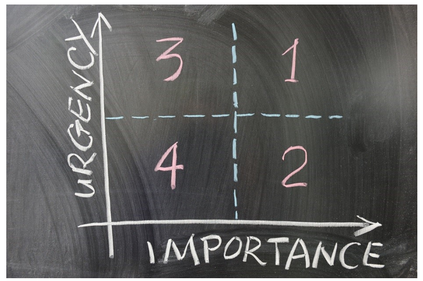
ISG QKD

Network architecture and security of quantum key distribution

Quantum Alliance Initiative

Security requirements, test and evaluation methods for quantum key distribution

Prioritize & Collaborate



1) QKD Key Interface
2) QKD Evaluation

UNIVERSITÉ DE GENÈVE

IDQ

Challenges Ahead

Quantum Supply Chain

Workforce with QT Skills

Security Evaluation

For more information

Eduardo.solana@unige.ch
Olivier.pfeiffer@idquantique.com

UNIVERSITÉ DE GENÈVE

IDQ

3rd CISO 360 CONGRESS 2019 Rome

Keynote Back from the future: What do the films Terminator, iRobot and Minority Report have to do with identity governance?

Ben Bulpett
EMEA Identity Platform Director, SailPoint

PULSE CONFERENCES

Back from the Future

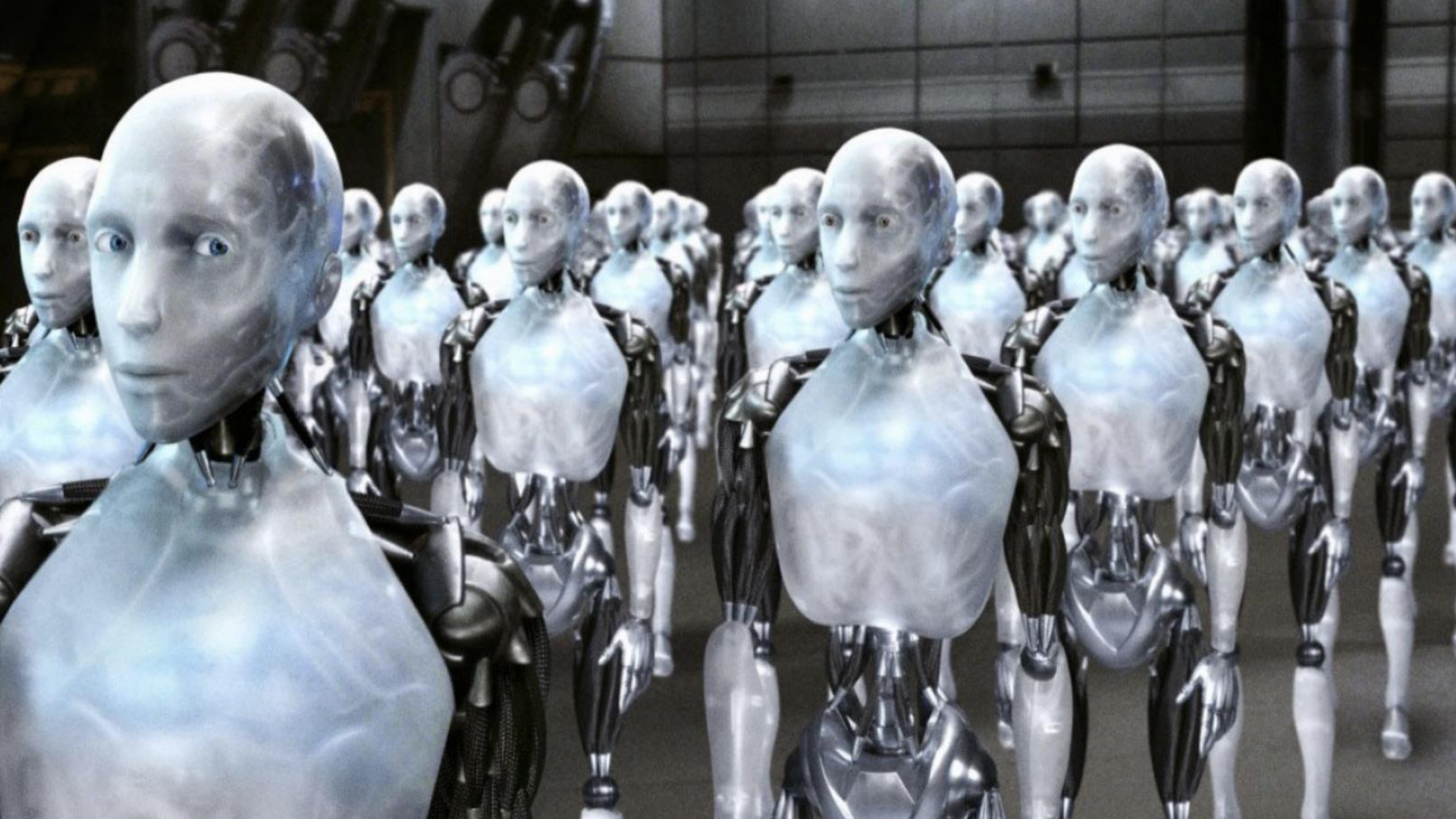
Ben Bulpett – EMEA Identity Platform Director


-16330,50
-6715,80
-18123,45
26740,18
-8488,74
-17786,46
-29748,09
-25257,23
31462,04
-6555,80
-27135,17
10272,69
1,568 %
4,833 %

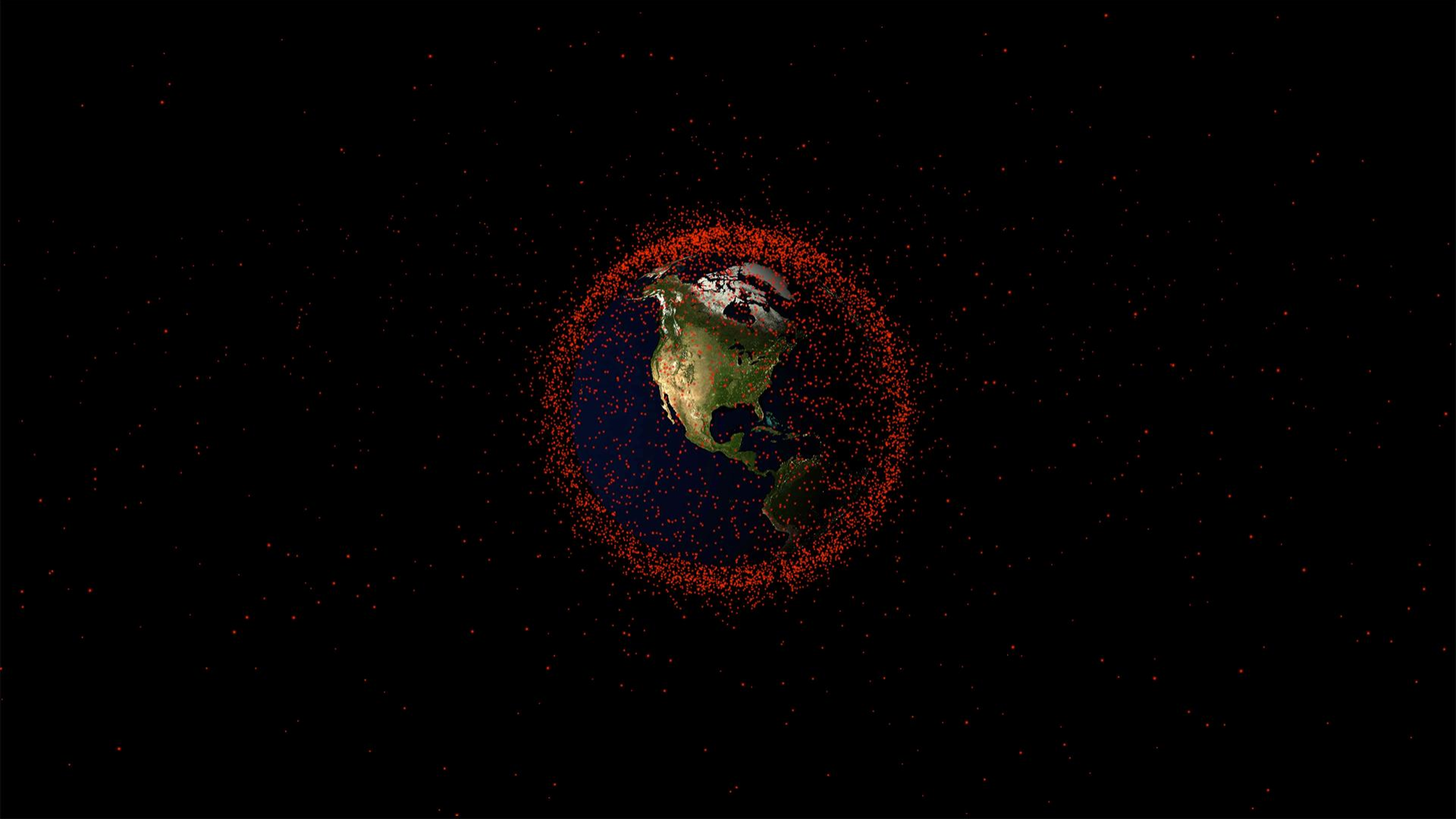

CSM-101

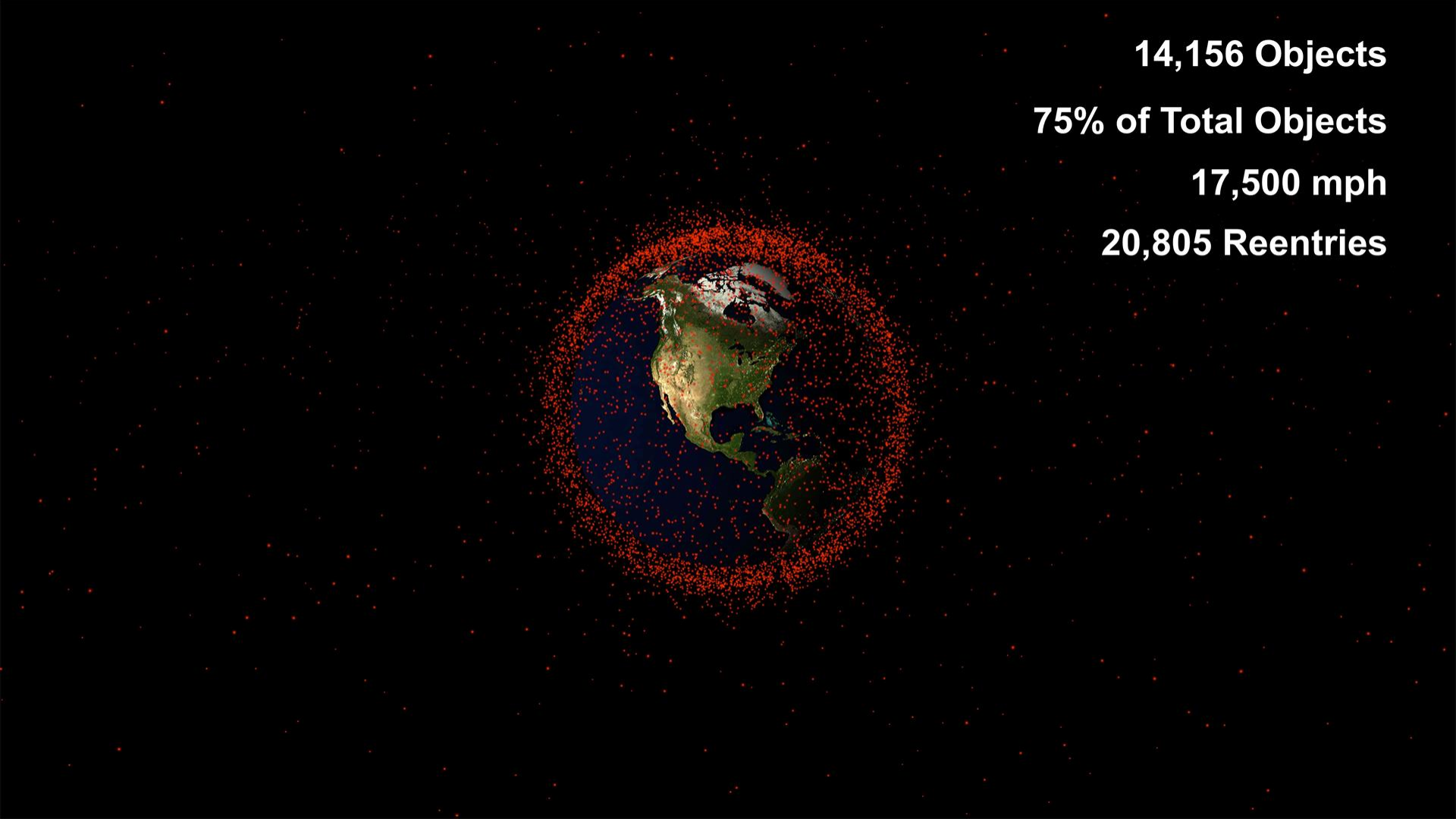

FEDERAL RESERVE NOTE
DF 08345533 A
F6
DF 08345533 A

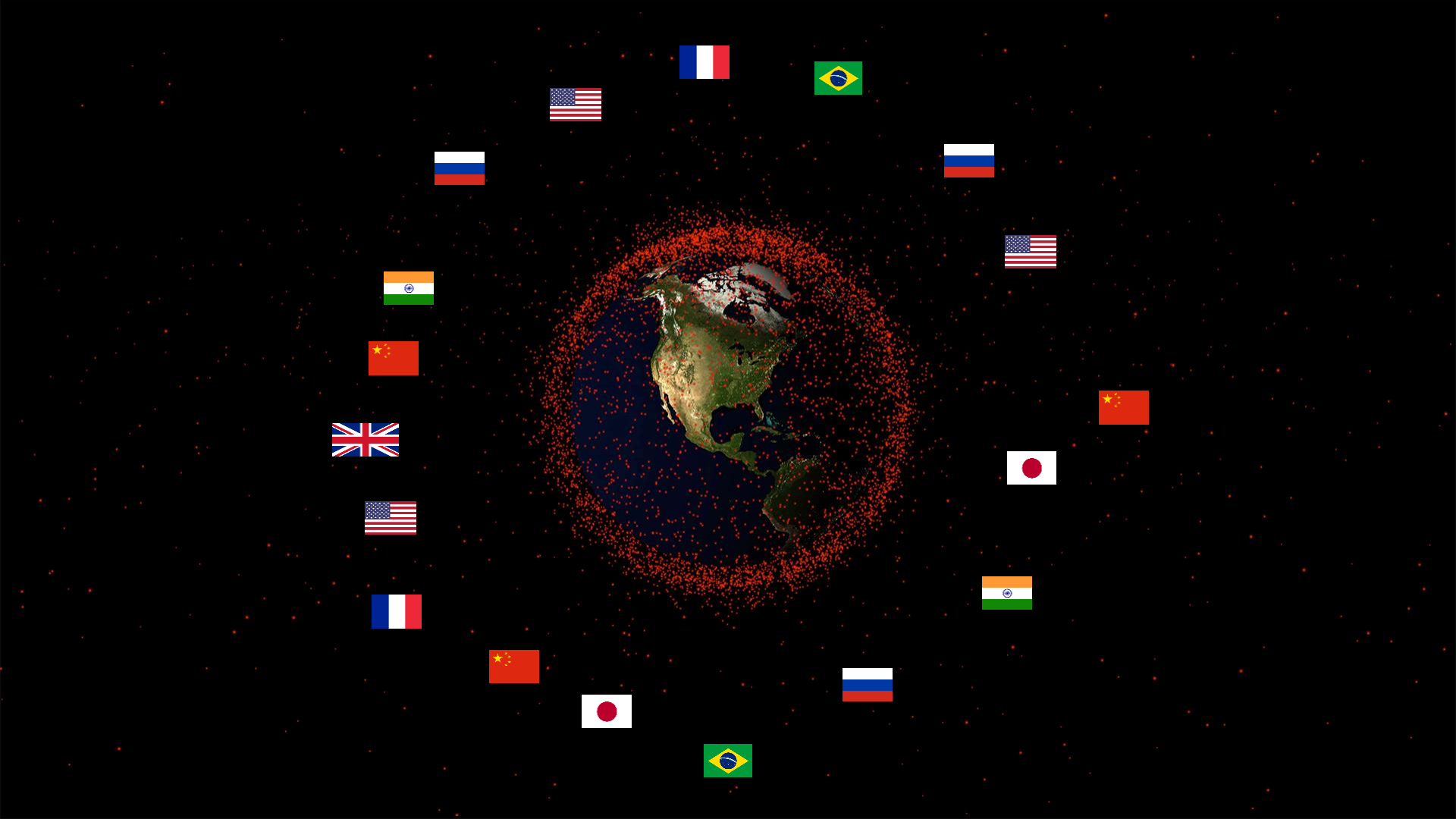

JAWS



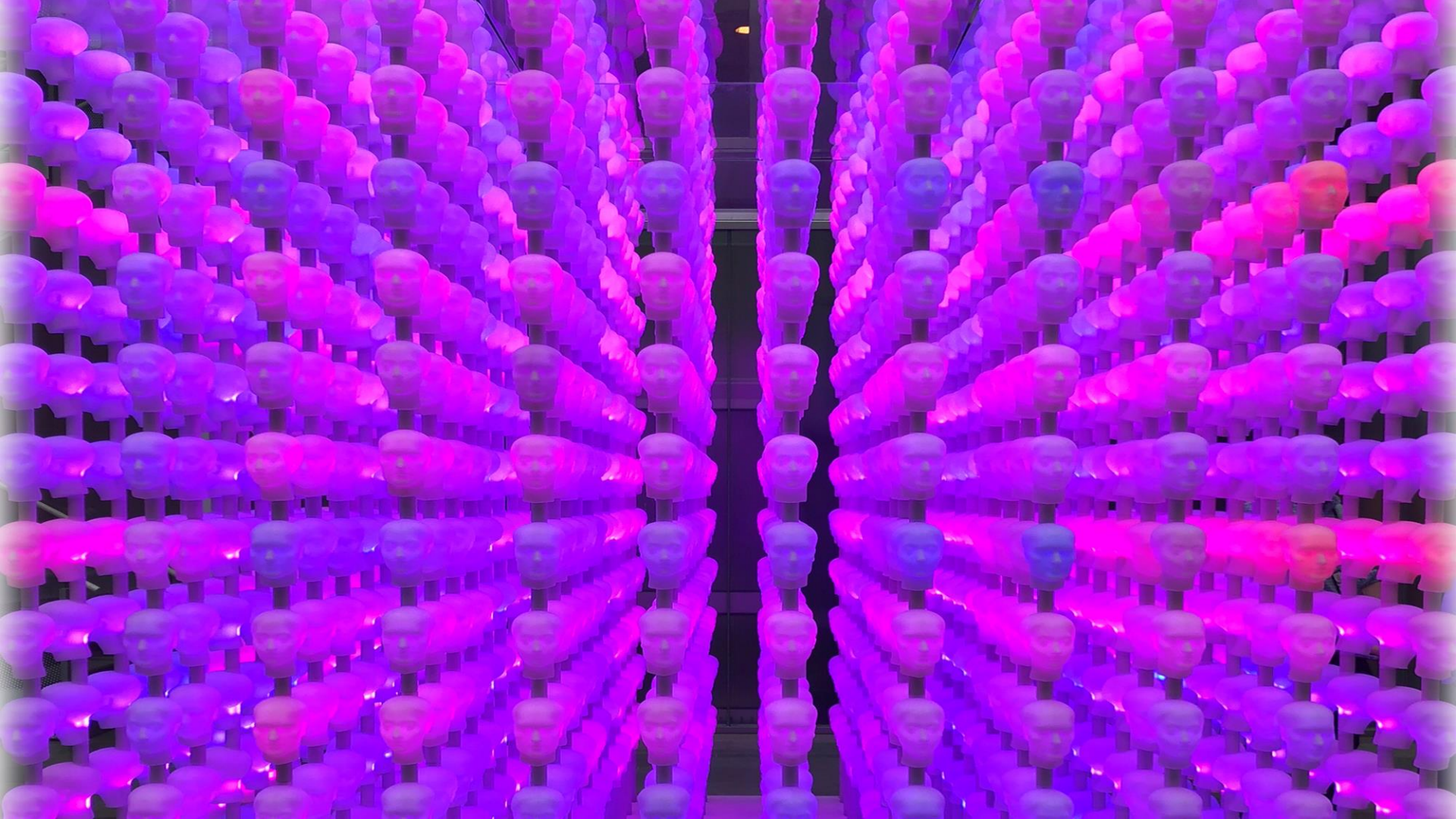

10%
25%
75%
40%
50%
100%



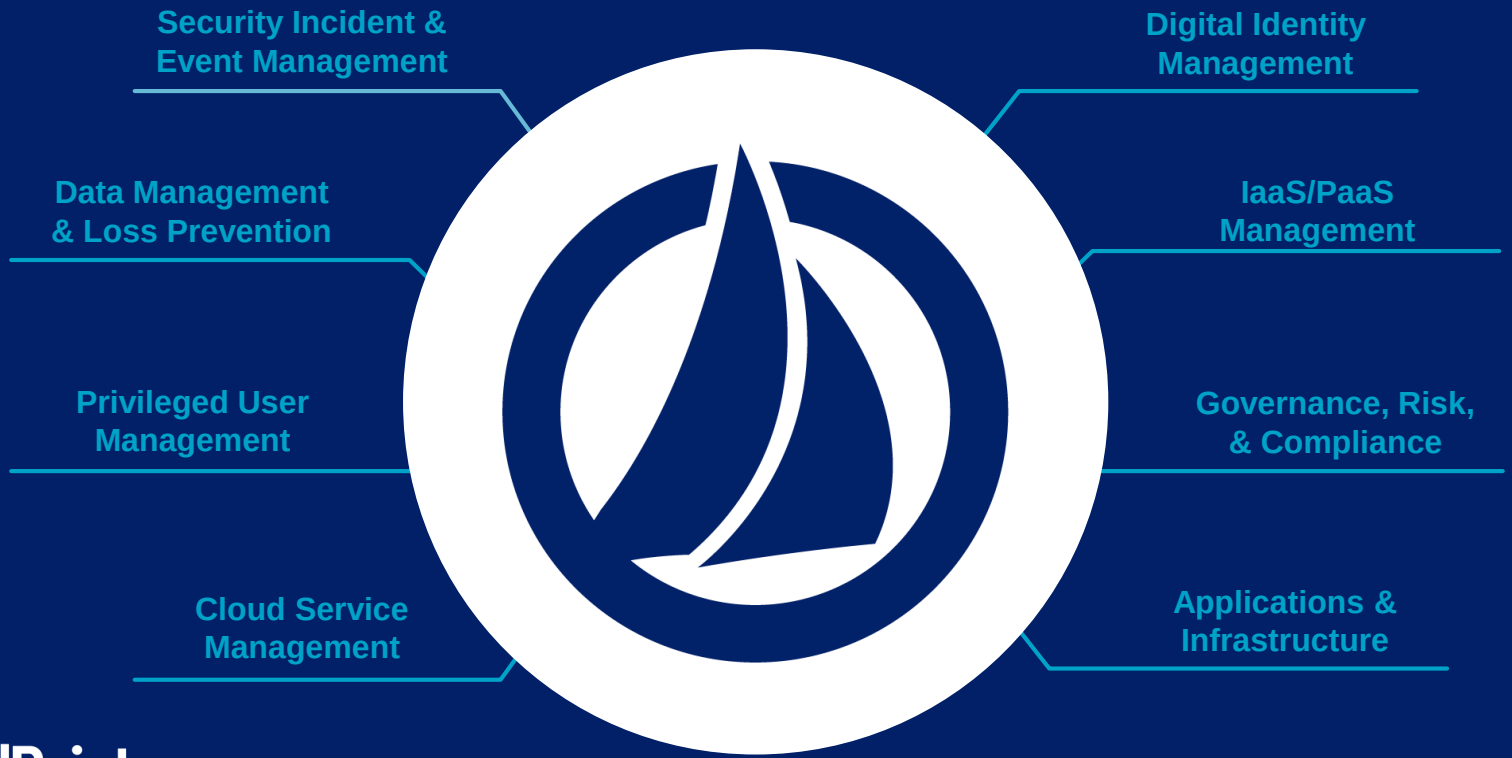

14,156 Objects
75% of Total Objects
17,500 mph
20,805 Reentries



Adjustable Equipment
Tether
00204178J



Identity at the Center of Transformation



SailPoint

Thank You

www.sailpoint.com

3rd CISO 360 CONGRESS 2019 Rome

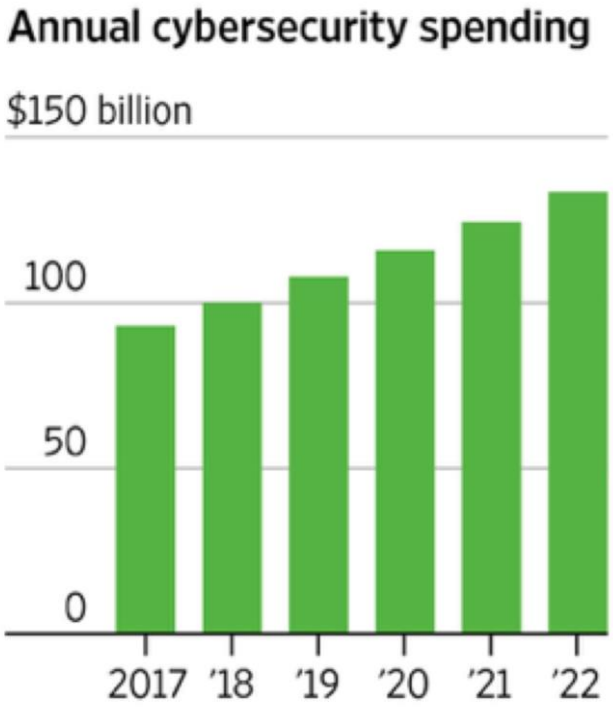
Keynote Balancing investment and security risk reduction

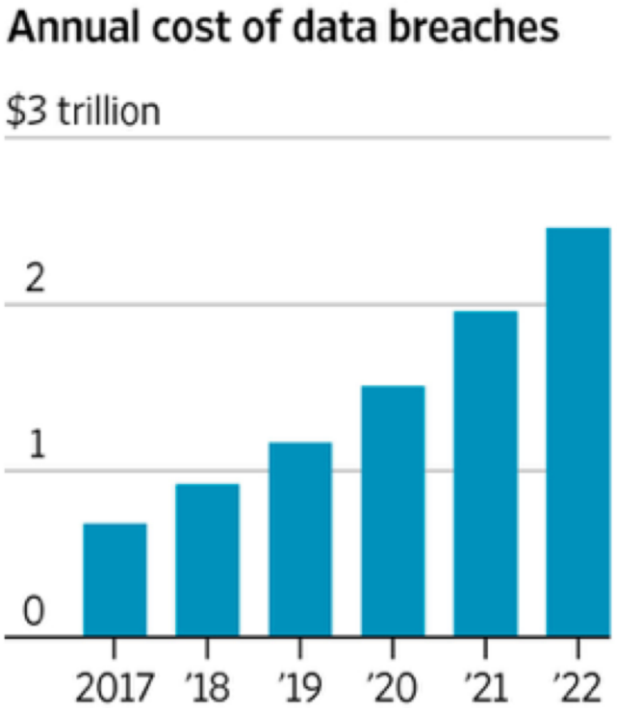
Mark Seddon
Director, CyberArk

PULSE CONFERENCES

BALANCING INVESTMENT & SECURITY RISK REDUCTION

DESPITE INCREASED INVESTMENT, ATTACKS GROWING IN FREQUENCY & COST





Source: Juniper Research/The Wall Street Journal

HOW MUCH??

We finally know how much a dat cost

People have been estimating the costs of data breaches for ye renegotiated Yahoo/Verizon deal, we finally have a real numbe

The big Bangladesh Bank heist: How hackers managed to steal $81 million

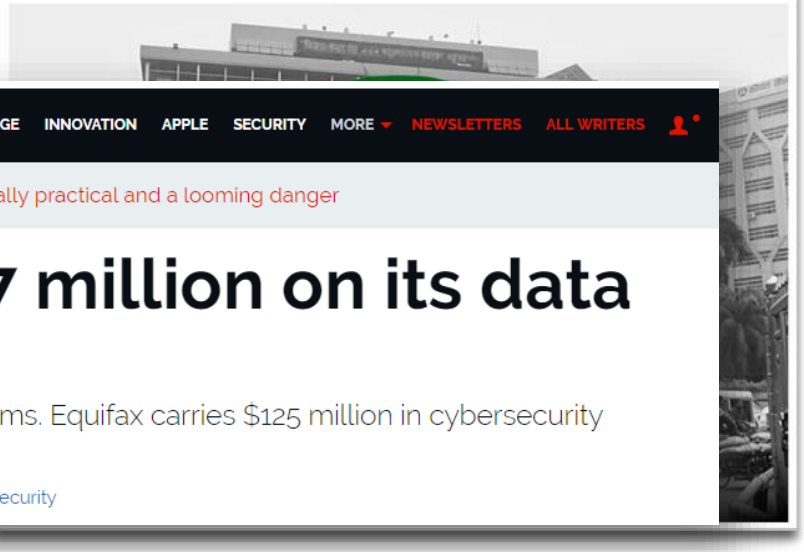
Posted on: 11:24 AM IST Mar 17, 2016

IBNLIVE.COM

21 More+

Bangladesh bank governor Atiur Rahman and two of the deputy governors have lost their jobs over the $81 million cyber heist that sent shockwaves through the banking world.

Now that more details are emerging it is becoming clearer how hackers managed to carry out one of the largest known bank thefts in history.



ZDNet

CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWSLETTERS ALL WRITERS

MUST READ: SHA-1 collision attacks are now actually practical and a looming danger

Equifax has spent $242.7 million on its data breach so far

The spending is shifting more toward data security and IT systems. Equifax carries $125 million in cybersecurity insurance with a $7.5 million deductable.

By Larry Dignan for Between the Lines | April 26, 2018 -- 07:00 GMT (08:00 BST) | Topic: Security

Increase in average cost of cybercrime over last 5 years

72%

Increase in average number of security breaches over last 5 years

67%

Security investments that produce negative value

55%

Source: 2017/2018 Cost of Cyber Crime Study. Accenture and Poneman Institute

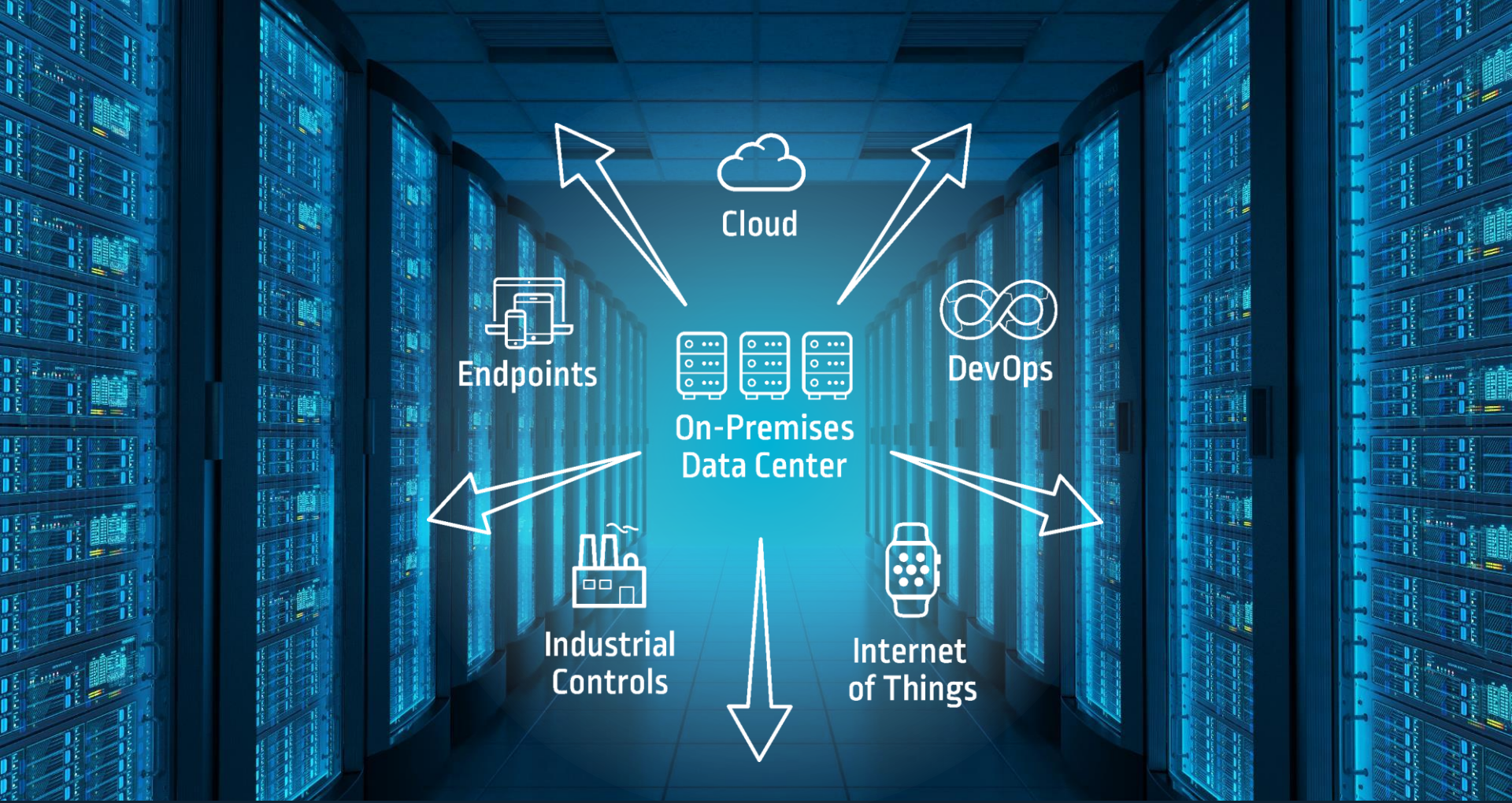
RISK

…effect of uncertainty on objectives
*- **ISO 31000***

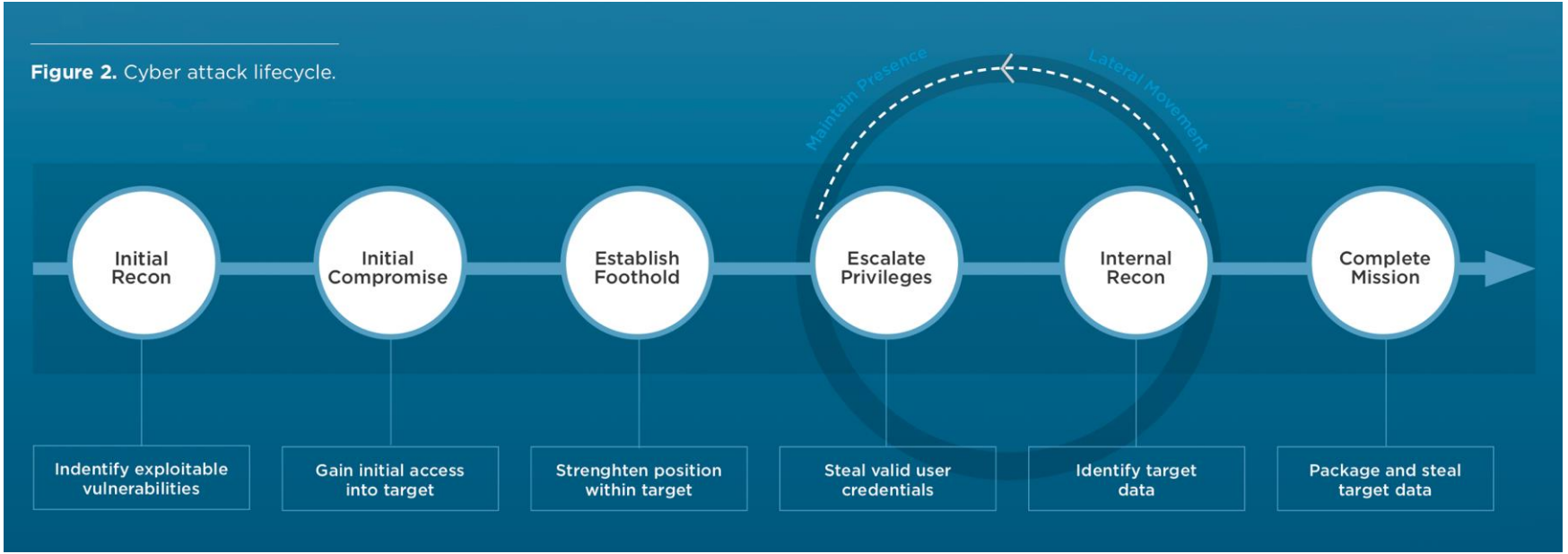
… the exercise of a threat against a vulnerability
*- **SANS***

*…a function of the **likelihood** of a given threat-source exercising a particular potential vulnerability, and the resulting **impact** of that adverse event on the organization*
*- **NIST** SP 800-30*


RISK =
THREAT x VULNERABILITY x CONSEQUENCE

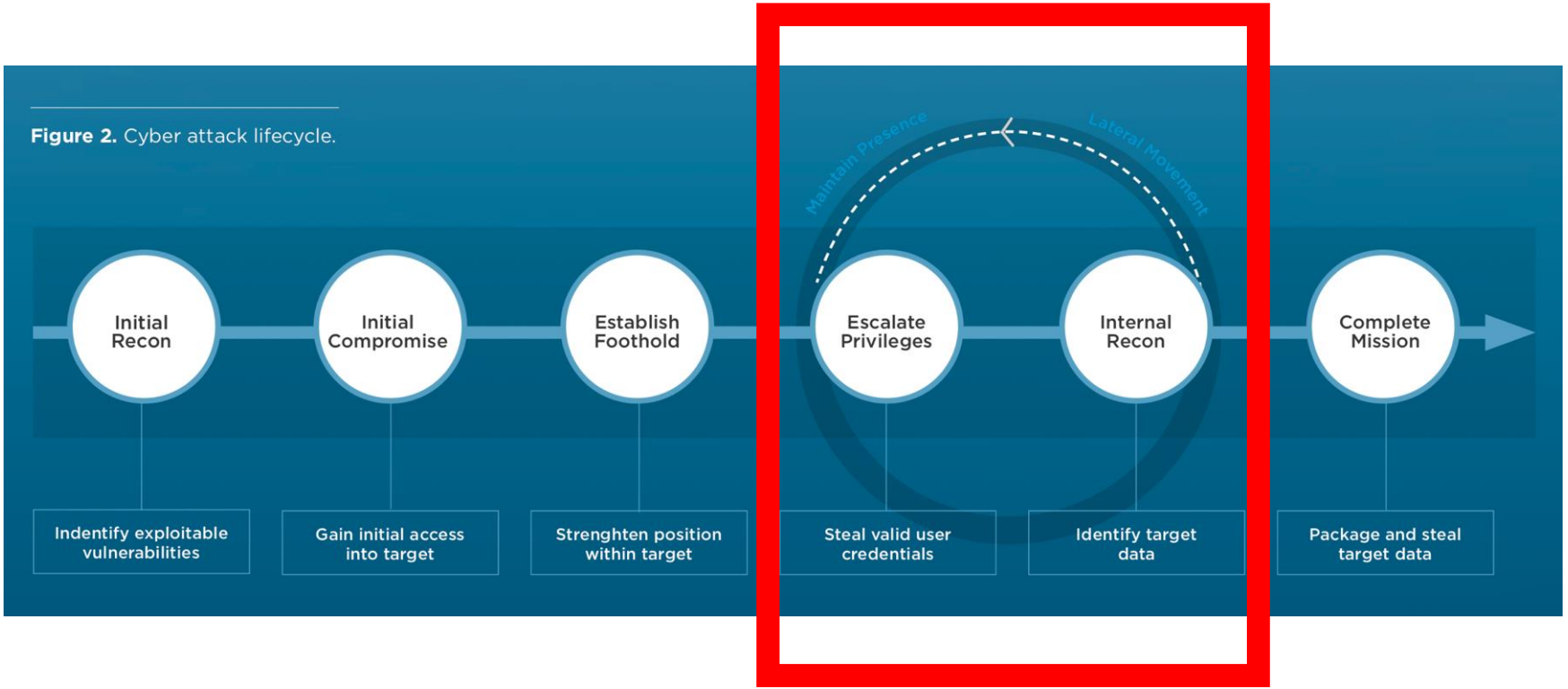

Cloud
Endpoints
DevOps
On-Premises
Data Center
Industrial
Controls
Internet
of Things

ANATOMY OF A CYBER ATTACK



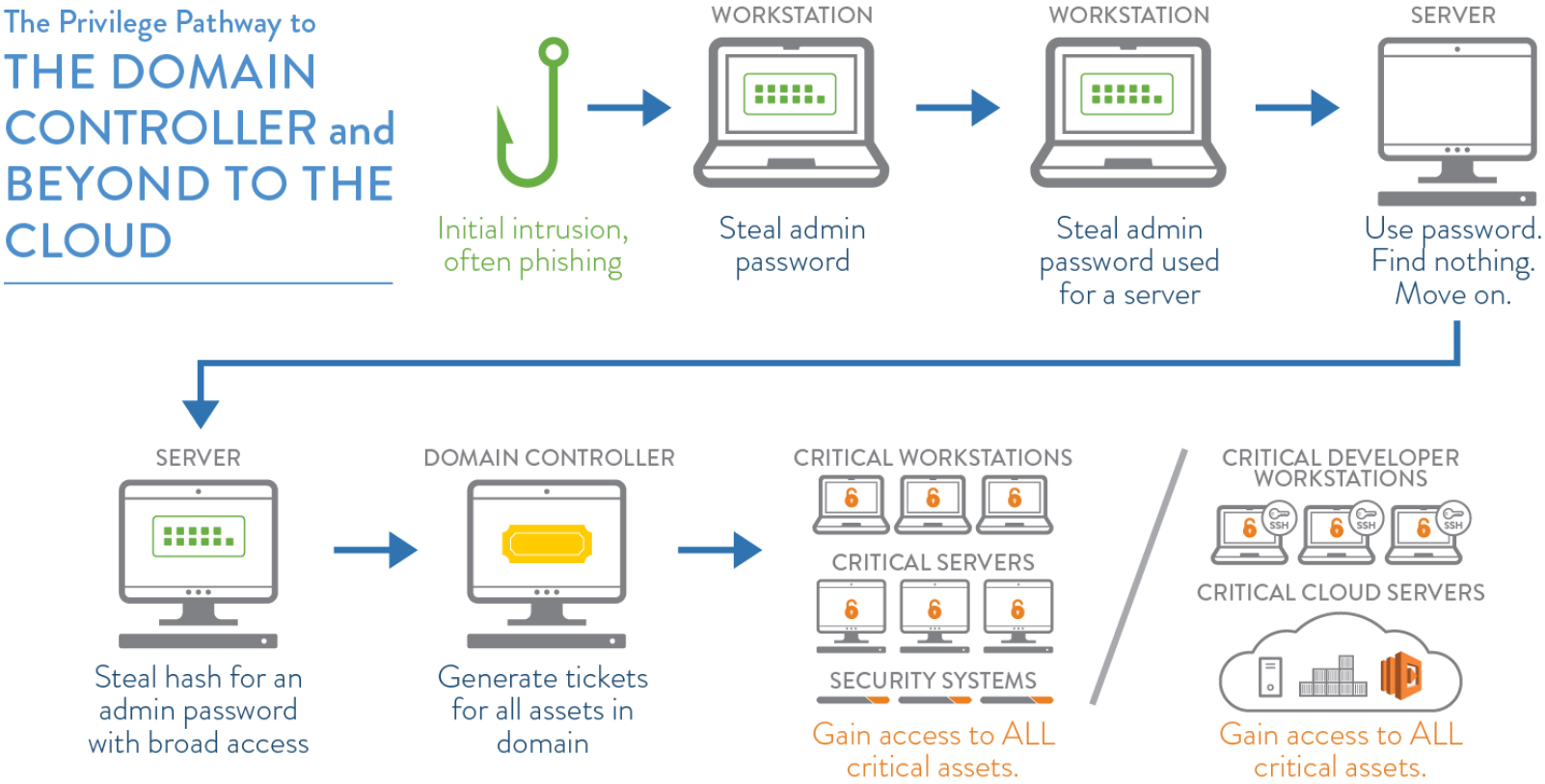
Source: Mandiant M-Trends

OBJECTIVES VARY, CREDENTIALS REMAIN WEAPON OF CHOICE



Source: Mandiant M-Trends

THINK LIKE AN ATTACKER - THE PRIVILEGED PATHWAY



FOR YOUR

CONSIDERATION

- Take a “Top-down” approach
- Rate and prioritize projects based on the business value delivered
- Measure business impact as Mitigation ROI or Return on Control
- Evaluate/adopt quantitative models such as FAIR and Hubbard Research
- Map Operational and Cyber Risk to identify maximum return

3rd CISO 360 CONGRESS 2019 Rome

Interactive Workshop Disruptive decision-making for CISOs - how people, process and partnerships contribute to transformation

---

Co-led by: Rob Robinson, Director of Security and Network Service, Company85
Paul Heffernan, CISO, Revolut (UK)

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Case Study 100 days as a CISO: Lessons learned from Scriptkiddie to CISO

Mark Snel
CISO - Information Security and Corporate Security, Signify (The Netherlands)

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Keynote Back to data security basics: What's getting lost in all the buzz?

Matt Middleton-Leal
GM EMEA & APAC, Netwrix

PULSE CONFERENCES

Back to Data Security Basics: What's Getting Lost in All the Buzz

Matt Middleton-Leal
Data Security Expert, Netwrix

Agenda

- Why is the data breach rate constantly going up?
- How are data security processes affected?
- What basic steps can help you strengthen data security?

Problem

DATA is the most valuable asset for any organization.

Financial documents

Healthcare records

Business plans

Cookie recipes

70%

Organizations say data growth is their top concern

88%

Is the expected increase in cybersecurity spending

52%

Data breaches were rooted in a human error or system glitch

The underlying reason

What is data security?

 Backups?

 Labels?

 VPN?

NO STAFF
NO TIME
NO BUDGET

+

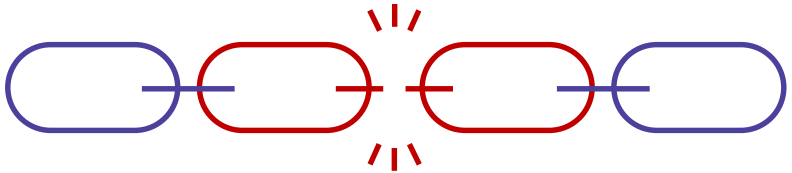
OVERCOMPLICATED
IMAGE OF
DATA SECURITY

=

RASH
CYBERSECURITY
DECISIONS

Real data security

Your organization is only as strong as its weakest link.



To find yours, see if you can answer these questions:

- What kinds of sensitive data do you have?
- What access rights do users have to sensitive data?
- What activity is going on around sensitive data?

Data Security Basics

1. Discover sensitive information

88%

Organizations store sensitive information in the cloud

88%

Businesses keep sensitive data in both databases and servers

53%

Employees store sensitive data on mobile devices

2. Classify your data

80% organizations don’t know what sensitive data they have

Public

Private

Restricted

3. Control who has access to what

74% employees have access to confidential information

Determine the level for access each individual

Establish and maintain a least-privilege model

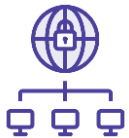
Disable accounts of departing employees promptly

4. Keep a close eye on what's going on

There's a cybersecurity attack every **39 seconds**

Look for spikes in user activity

Check activity outside of business hours

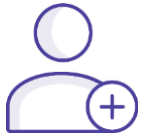


Control anomalous VPN access

5. Make data security a continuous process

800% data growth in data volume is expected by 2022

Threat landscape is evolving



Internal conditions are changing

Data is dynamic

LESSON LEARNED

GET BACK TO BASICS

Questions?

Thank You!

3rd CISO 360 CONGRESS 2019 Rome

PERSONAL Keynote What is the true cost of security?

Thomas Langford
Information Security Advisor, Comic Relief (Frmr CISO, Publicis Groupe) (UK)

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

WHAT IS THE TRUE COST OF SECURITY?

A personal story

(TL)2 SECURITY

@thomlangford
@tl2security


@thomlangford
@tl2security


@thomlangford
@tl2security


Whatever you do today, do it with the confidence of a four year old in a **Batman t-shirt**.
@thomlangford
@tl2security

THANK YOU

thom@tl2security.com

uk.linkedin.com/in/thomlangford

@thomlangford
@tl2security

(TL)2 SECURITY

3rd CISO 360 CONGRESS 2019 Rome

3rd CISO 360 CONGRESS 2019 Rome

Keynote DNS: Cyber security's best kept secret

Ben Jeffreys
Senior Executive, Nominet

PULSE CONFERENCES

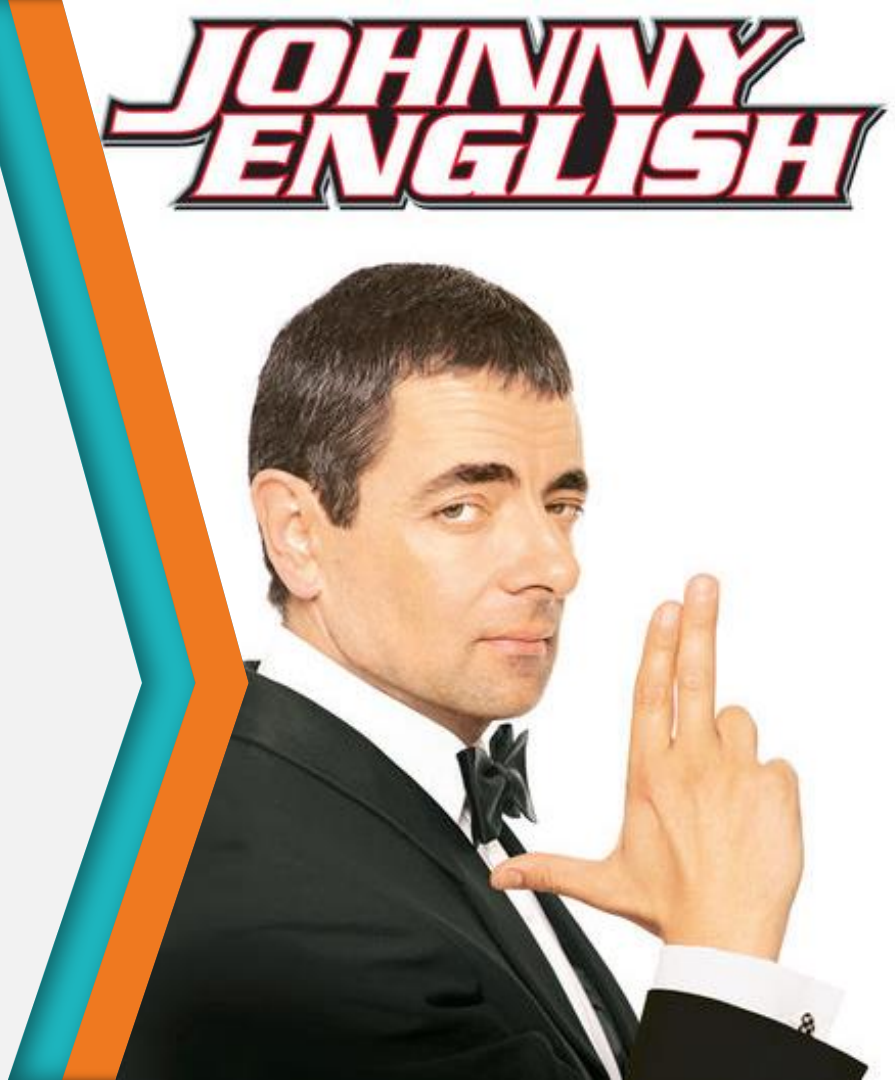
3rd CISO 360 CONGRESS 2019 Rome

Unique Keynote Threat from Business Espionage

Robert Shaw
Senior Security Advisor, United Nations (UK)

PULSE CONFERENCES

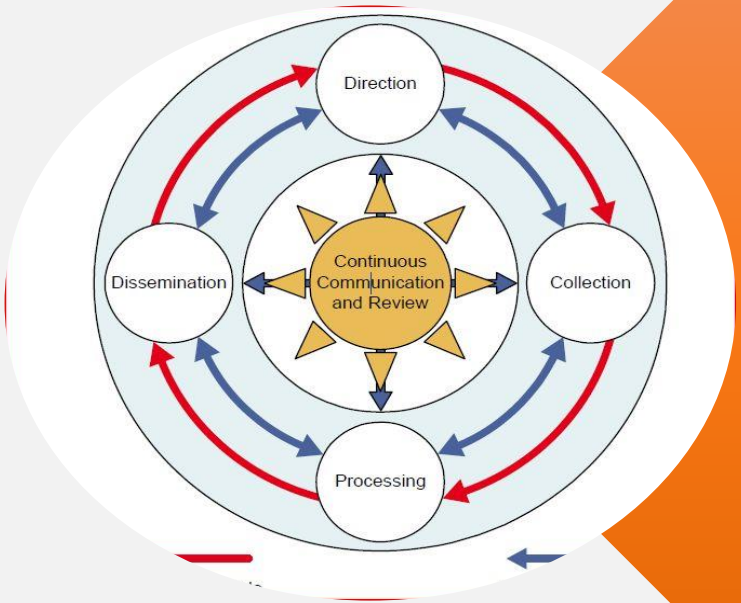
Business Espionage



Robert Shaw
info@teg7.co.uk

Member of The Exercise Group 7, TEG7 LLP
Member of the Register of Security Engineers and Specialists
www.TEG7.co.uk

WHAT IS INTELLIGENCE?



- Information that is processed.
- Not done for the sake of it. RFI.
- Direction-Collection-Processing- Dissemination.
- Not good at psychological and cognitive aspects.
- Timeliness

LEVELS OF INTELLIGENCE

- Strategic/Operational/Tactical
- Tactical doesn't mean unimportant. Access?

HOW IS INTELLIGENCE COLLECTED?

- SIGINT-Mobile/Wifi
- EXPLOITATION-TECHINT-Reverse engineering
- MASINT-Jet engines
- IMINT-Drone/Street view
- OSINT-Social Engineering/Street view
- HUMINT-CHIS
- All commercially available systems!

HOW IS INTELLIGENCE COLLECTED?

- Technical or HUMINT
- HUMINT-Cheaper?-Primary or Access
- Graded and Cross Referenced

BUSINESS INTELLIGENCE

- Government and Business Intelligence blurred.
- Is collected because it provides an advantage.
- Will use collection methods based on costs/risk appetite/Law.
- Usually OSINT/HUMINT-Legal/Cheap.

COUNTER INTELLIGENCE AND SECURITY

- Prevention of intelligence gathering is through understanding the threat- generic and specific.
- Most generic security processes will help.
- Monitoring of personnel will identify the insider threat. Interface with HR.

THE INSIDER THREAT

- Disgruntled Employee.
- Money/Ideology/Coercion/Ego-Unhappy/Fired.
- Damage done on leaving.
- Unwitting
- No loyalty?-Employment Model

CASE STUDIES

- Aircraft Manufacturer
- RFI-Technical Plans. Save R&D costs-Billions
- Security good-sub contractor
- False Flag recruitment and Money
- Well within commercial means

CASE STUDIES

- Defense Supplier
- No security personnel
- False Email
- 1.8 million
- Money transferred and taken from ATM's

CONCLUSION

- Its not just about an organization but understanding of its culture and the marketplace
- CI-Understanding the threat and creation of a security culture
- Procedures and staff training-become routine
- CI-Constant training/Red Teaming/Penetration Testing
- Security can be the cheapest bidder!
- Int collection and security technology changes but humans will always be the weakest link

QUESTIONS

- QUESTIONS?

3rd CISO 360 CONGRESS 2019 Rome

Case study Cloud journey

Marc Lueck
CISO, Zscaler

PULSE CONFERENCES

Cloud and Security – Get Ahead of the Curve

Marc Lueck

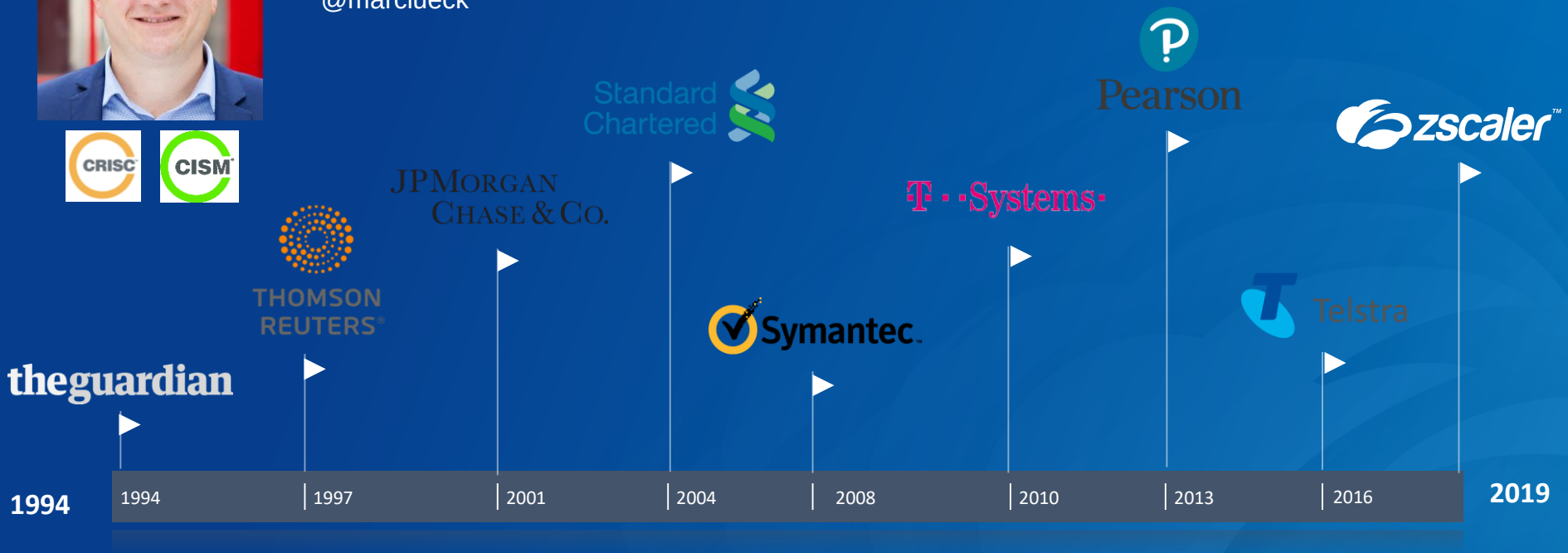
19 June 2019

A Little About Me

Marc Lueck
CISO UK & Northern Europe
@marclueck

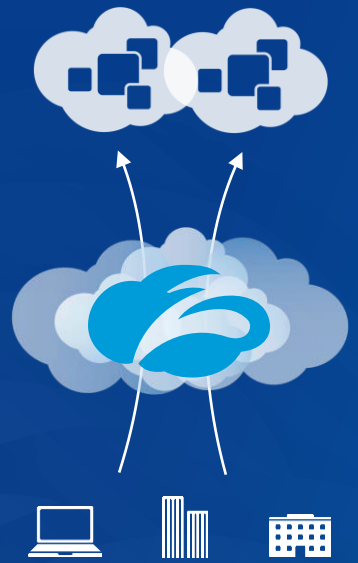
CRISC CISM

24 Years delivering security to companies or customers



Zscaler: Securely transform IT for a cloud world

Business policies connect users to apps
from anywhere, over any network



FAST. SECURE. RELIABLE.

Market Leader **300** of the **Forbes Global 2000**
Nasdaq: ZS

Global Presence **100+** **data centers** across 6 continents

Proven Scale **65B+** **transactions** processed daily

Cloud and mobility: enablers, but disrupt networking and security

Old World

New World

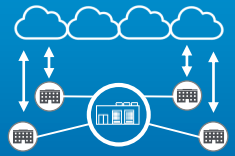
It started with cloud app adoption…

DC

Cloud + DC

And that drives network transformation…

Hub-and-Spoke to DC



Direct-to-Cloud

Which disrupts network security

Network Security

RISK?

The security industry is still trying to resolve this

81% of organisations polled report that the maturity of their cloud security strategy is at the median or lower.

ClubCISO Security Maturity Report 2019

We have to reset the clock on cloud security strategies several times a year. Every year when we ask this question we seem to go backwards.

ClubCISO Member – Live Vote March 2019


“Digital transformation is like a big wave….
You can’t stop it, but you can learn how to surf !!”
F.Janssen – Director, IT Service Portfolio at Siemens

What can we do?

1 Gain Visibility

Understand what the business wants
See what the business is doing

2 Enable the Cloud

Meet the business needs for services
Provide service securely, on your terms

3 Secure Cloud Compute

Build your cloud compute strategy
Be ready to compromise

1

Gain Visibility into Business Cloud Use and Strategy

Knowledge is Power

> Visibility creates order from chaos
>
> Marc Lueck – CISO360 Congress
> Rome, June 2019

Visibility is the seed to future compliance:

- Policy must work for the business – not the other way around
- With clear understanding of business practices, policy can be adjusted to suit the business
- Ongoing visibility is a key component for future enforcement & compliance

2

Adjust Policy to Enable Your Business

Enabling the Cloud – Get involved

Controls based	→	Risk based
No you can't	→	Yes… and here's how
Build services	→	Create value
Prevention	→	Detection and response
Requirements	→	Innovation – fail fast
Network-centric	→	User-centric

3

Secure your future path to cloud compute

Cloud Compute – still a real area of unmanaged risk

Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall

Client-side encryption implementation, Server-side encryption, Network Traffic Protection

Security in the cloud

AWS Foundation Services

Compute | Storage | Database | Networking

amazon web services

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Security of the cloud

Securing Cloud Compute

It’s still a policy issue

- Build a control matrix
- Controls are not technology, they are outcomes!
- Understand equivalence, vs. exporting your old security to the cloud
- Consider turning your cloud compute environment “dark”
- Extend and validate your trust – move from Implicit to Explicit trust

Manage Measured Risk – Not Perceived Risk

3rd CISO 360 CONGRESS 2019 Rome

Panel How do we build a successful culture of security, privacy and trust? Navigating complex regulatory oversight to ensure ethics and compliance

---

Chaired by:
David Cripps, Frmr CISO, SETL and Investec (UK)
Panellists:
Colette Hanley, Chief Privacy Officer, Nokia (UK)
James Gosnold, Head of Cyber Technology Services, UK Department of Work and Pensions
Martyn Booth, CISO, Euromoney Institutional Investor PLC (UK)
Mark Felegyhazi, CEO, Avatao; Rob Robinson, Director of Security and Network, Company85 (UK)
Lee Cartmell, Group CISO, Stagecoach Group (UK)
Matt Middleton-Leal, GM EMEA & APAC, Netwrix

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

LEAD QUESTIONS: Panel How do we build a successful culture of security, privacy and trust? Navigating complex regulatory oversight to ensure ethics and compliance

---

Privacy is becoming an ever-increasing concern in the world. Social Networks, GDPR and on the opposite end of the spectrum, China's Social Credit System. Where's the boundary of security and privacy?

- Realities of the new privacy regime GDPR
- How to win hearts and minds - culture versus training
- Measuring effectiveness - what KPIs work?
- Can regulatory frameworks alone build trustworthiness?
- How do you build organisational accountability?
- How can we demonstrate trustworthiness?
- Who do we trust today and why? Can trust be absolute or does it depend on context?
- Can you recover from a breach of trust/trust deficit? How?
- How do organisations sabotage trust? How can we innovate yet maintain trust?
- Does trust matter if people still buy our product?

PULSE CONFERENCES

3rd CISO 360 CONGRESS 2019 Rome

Developed and Hosted by

PULSE CONFERENCES

Close of day One

Join us for Networking Reception and Dinner

18:15 Coaches Depart from the Radisson Blu for the Reception - Borgo Ripa Gardens Rome

Dinner - Taverna De' Mercanti Rome

Coaches Depart from Radisson Blu Hotel: 18.15

Platinum

TELSTRA

Gold

Company85 accomplish more · SailPoint · CYBERARK · BITSIGHT · BARCLAY SIMPSON · NOMINET · AGARI · ExtraHop Rise Above the Noise. · netwrix · DARKTRACE · zscaler · RISKIQ · OneTrust Privacy Management Software · proofpoint

Silver

SOC PRIME · Synack · Fidus · CyberCyte

Bronze

CHECKMARX

Lunch Sponsor

IDECSI Enterprise Security

Panel Sponsors

GARRISON · avatao Learn to build secure software · NetClean

Exhibition Sponsor

GURUCUL

Supporting Associations

ISACA Rome Chapter