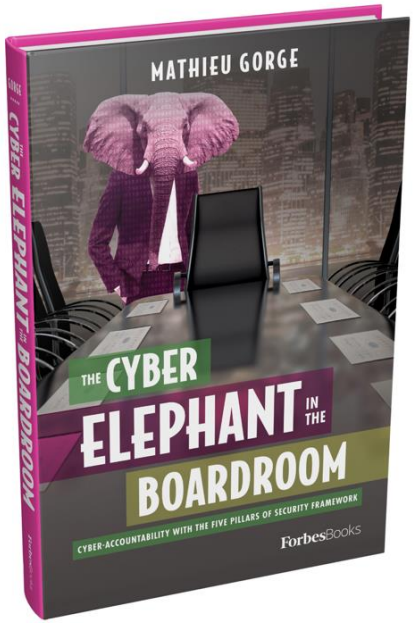


VIGITRUST

Most Influential Business Leaders in CYBER Security 2022

Integrated Risk Management SaaS Provider

Global Privacy Day 2023

mathieu.gorge@vigitrust.com

https://ie.linkedin.com/in/mgorge

Europe Edition

Hall Of Fame 2022

VIGITRUST

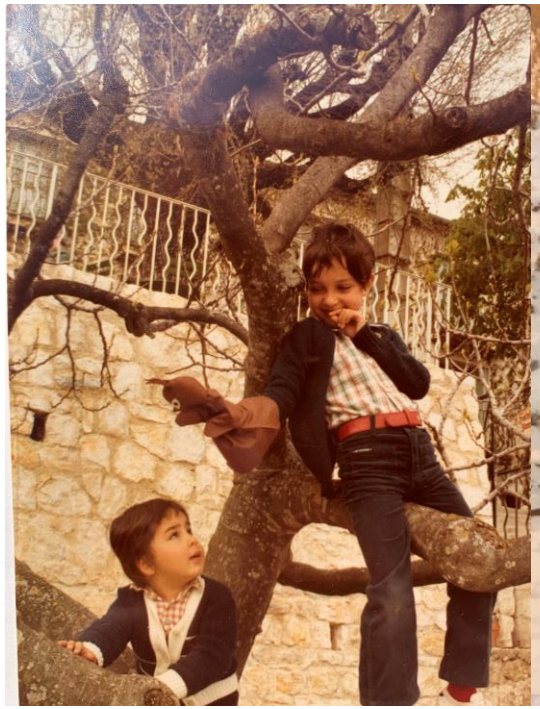
Helping Companies to Prepare, Validate and Comply

Mathieu Gorge
Founder and CEO, VigiTrust

Disclaimer before we all fall out…..

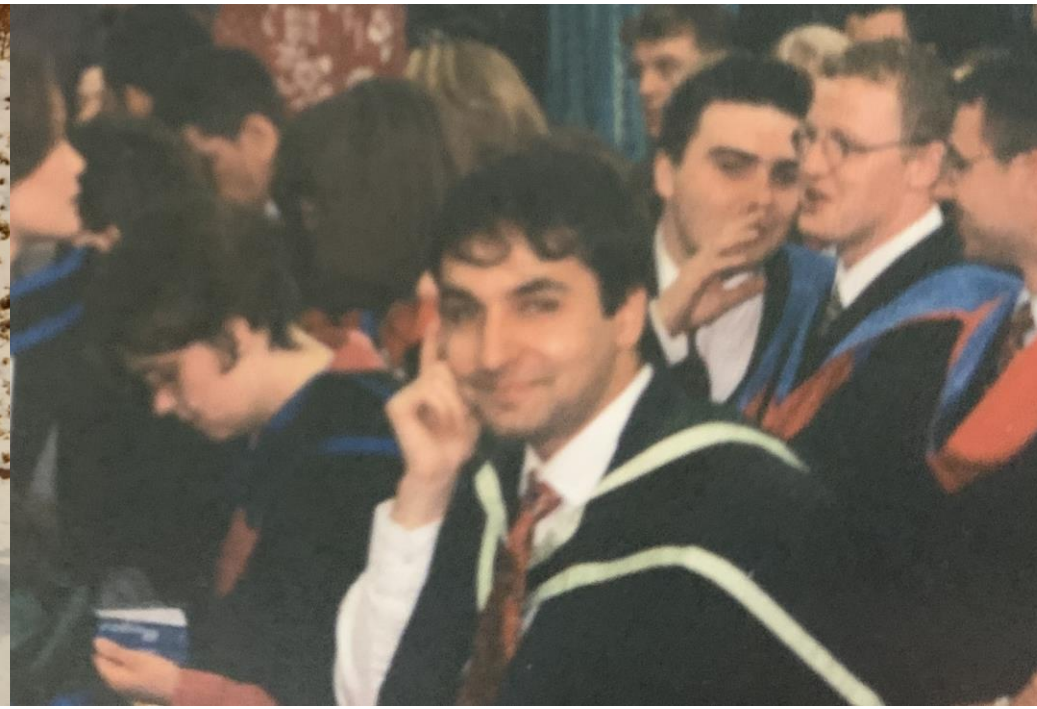
I’m a man and I’m French ….so I’m definitely going to say something wrong ☺

My views on privacy have changed throughout life because of…



Culture & Family

Early Education



University & early Jobs

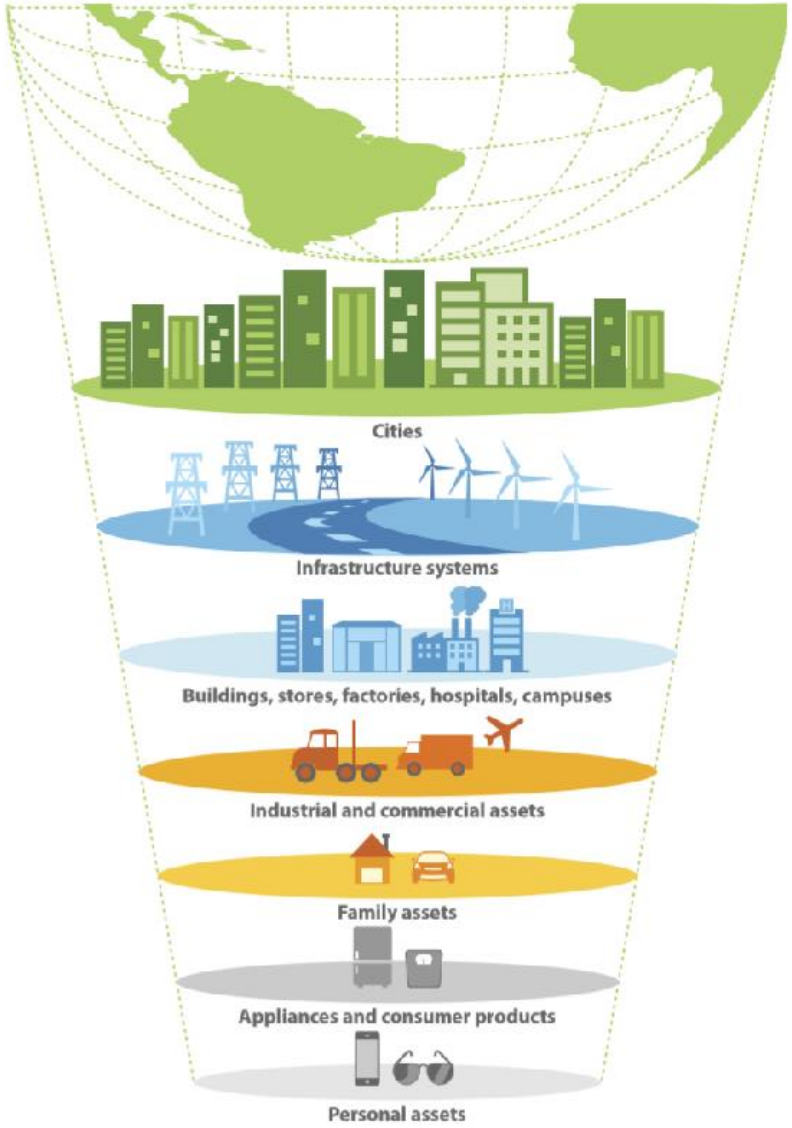
Critical Infrastructure Considerations – Impact on personal and business data footprint

CI Perspective

- electricity generation and distribution
- telecommunication
- water supply
- agriculture, food production and distribution
- heating (natural gas, fuel oil)
- public health
- transportation systems (fuel supply, railway network, airports)
- financial services
- security services (police, military)

Basic concepts and assumptions

- Citizens take critical infrastructure as a given
- Businesses do not think pro-actively about their dependence on critical infrastructure
- Would be terrorist are looking for ways to exploit these gaps



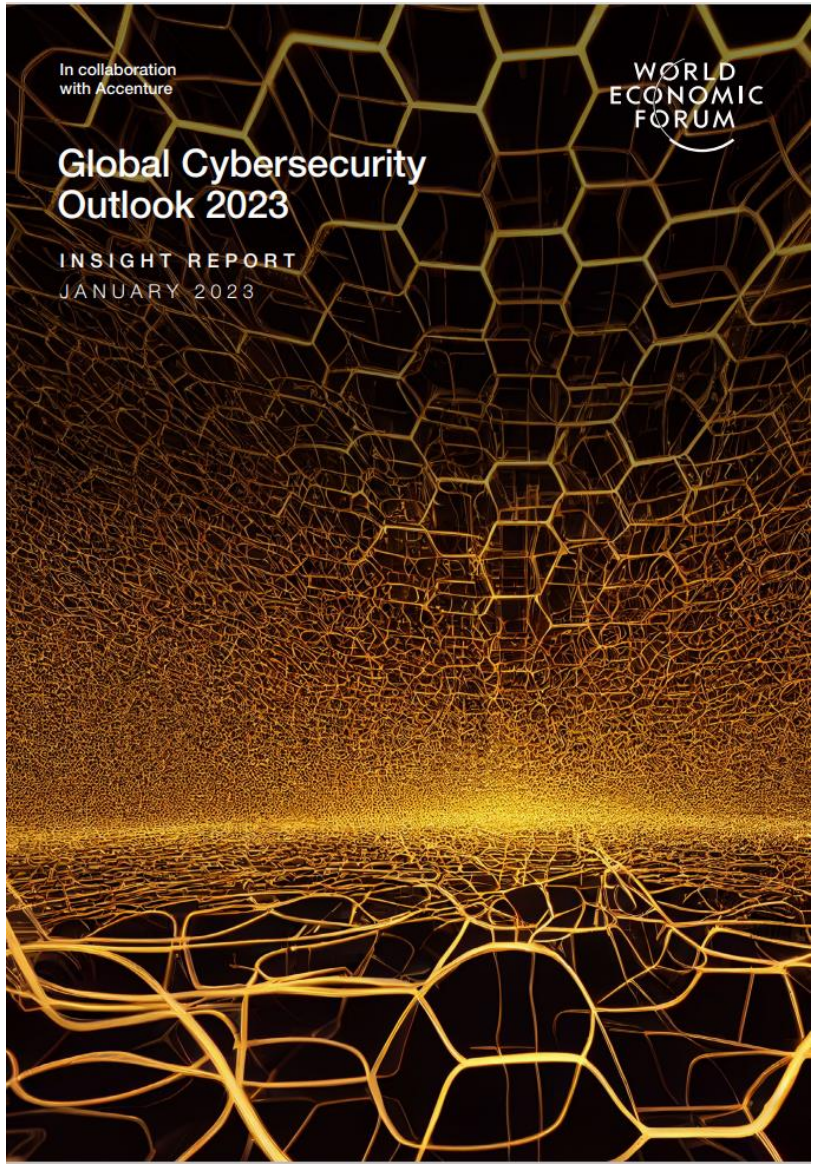
Top Short-Term Global Risks

Over the next 0-2 years

FAIL

Global Risks Report 2022

Image: World Economic Forum



Cover: Artwork created using artificial intelligence, prompt, art direction and refining by Studio Miko
Images: Getty Images

Contents

- The character of cyberthreats has changed. Respondents now believe that cyberattackers are more likely to focus on business disruption and reputational damage. These are the top two concerns among respondents.

- Global geopolitical instability has helped to close the perception gap between business and cyber leaders' views on the importance of cyber-risk management, with 91% of all respondents believing that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.

- Following from this, 43% of organizational leaders think it is likely that in the next two years, a cyberattack will materially affect their own organization. This, in turn, means that in many cases, enterprises are devoting more resources to day-to-day defences than strategic investment.

- The data protection and cybersecurity concerns created by geopolitical fragmentation are increasingly influencing how businesses operate and the countries in which they invest.

- Structured interactions between cyber and business leaders are becoming more frequent – 56% of security leaders now meet monthly or more often with their board. This is rapidly narrowing the cybersecurity perception gap. However, more needs to be done to promote understanding between business and security teams to support effective action by organizational leaders.

- Building a security-focused culture requires a common language based on metrics that translate cybersecurity information into measurements that matter to board members and the wider business.

- Changes in organizational structure that embed cyber-risk discussions across a business can also promote more fluid communication and effective cyber-risk management.

- Ultimately, cyber leaders must present security issues in terms that board-level executives can understand and act on. Business leaders, for their part, need to accept more accountability for operational cyber requirements to advance their organizations' overall cyber capabilities.

IAPP Privacy Perspectives

Key Dates from US Comprehensive State Privacy Laws

iapp

LEGEND

CALIFORNIA
- **CCPA** – California Consumer Privacy Act
- **CPRA** – California Privacy Rights Act
- **CPRA** – CPRA Ballot Initiative
- **CPPA** – California Privacy Protection Agency

VIRGINIA
- Virginia's Consumer Data Protection Act

COLORADO
- Colorado Privacy Act

CONNECTICUT
- Connecticut Personal Data Privacy and Online Monitoring Act

UTAH
- Utah Consumer Privacy Act

2020

JAN. 1, 2020
CCPA effective date.

JULY 1, 2020
CCPA enforcement date.

2021

2022

JAN. 1, 2022
CPRA look-back period begins (CPRA Ballot Initiative Section 31(a)).

JULY 8, 2022
CPPA begins formal rulemaking process to update existing **CCPA** regulations and adopt new regulations.

2023

JAN. 1, 2023
CPRA, which amends the CCPA, becomes fully operative. No longer a right to cure (CPRA Ballot Initiative Section 31(a)).

Operative **CPRA** employee and business-to-business exemptions expire (CPRA Sections 1798.145(m) and (n)).

JAN. 1, 2023
Virginia Law's effective date.

JULY 1, 2023
Colorado law's effective date (Section 7).

JULY 1, 2023
CPRA enforcement begins (CCPA Section 1798.185(d)).

JULY 1, 2023
Connecticut law's effective date.

2024

DEC. 31, 2023
Utah law's effective date (Section 17).

JULY 1, 2024
Colorado's law requires universal opt-out mechanism (Section 6-1-1306(1)(a)).

2025

JAN. 1, 2025
Connecticut deadline for controllers to allow a consumer to opt out through an opt-out preference signal (Section 6(e)(1)(A)(ii)).

Connecticut right to cure expires (Section 11(b)). Attorney general has discretion to grant cure period (Section 11(c)).

JAN. 1, 2025
Colorado notice of violation and right to cure expires (Section 6-1-1311(1)(d)).

Global Risk Landscape

Geopolitical Impact – Russia& Ukraine

What does Mustard have to do with Global Supply?

USDA U.S. DEPARTMENT OF AGRICULTURE

GLOSSARY ASKUSDA RECALLS CONTACT US

HOME TOPICS OUR AGENCY MEDIA

USDA › MEDIA › PRESS RELEASES › USDA WILL PARTNER WITH UKRAINE TO STRENGTHEN AGRICULTURAL COLLABORATION AND FI...

- Agency News Releases
- Agency Reports
- Blog
- Digital
- **Press Releases**
  - Press Release Archives
- Radio

Share Feedback

USDA will Partner with Ukraine to Strengthen Agricultural Collaboration and Fight Global Food Insecurity

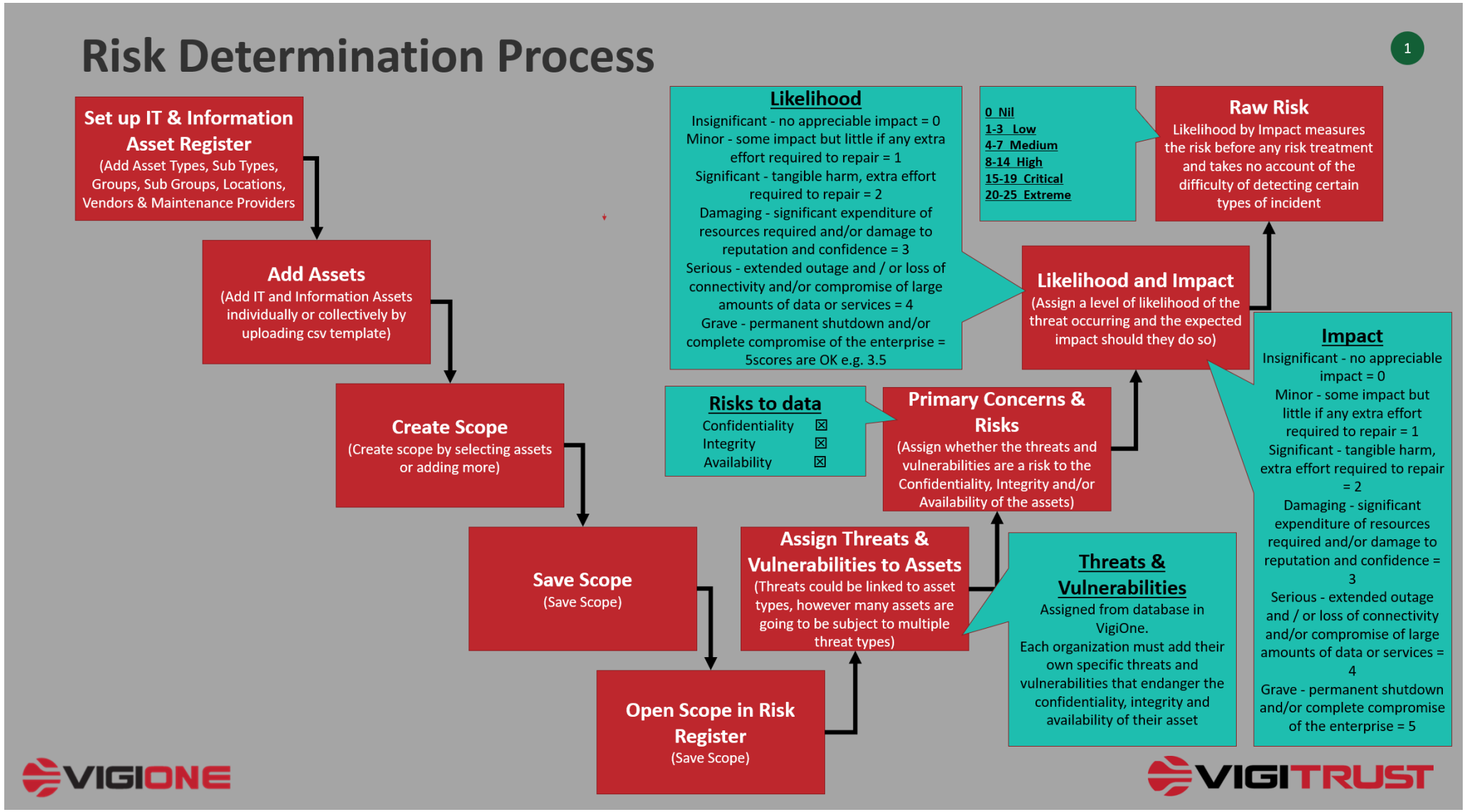
Press Release
Release No. 0132.22

Contact: USDA Press
Email: press@usda.gov

NEW YORK, June 16, 2022 – Today during a meeting with U.N. ambassadors and officials at the U.S. Mission to the U.N., United States Secretary of Agriculture Tom Vilsack announced the U.S. Department of Agriculture (USDA) and The Ministry of Agrarian Policy and Food of Ukraine are entering into a Memorandum of Understanding (MOU) to enhance coordination between the U.S. and Ukrainian agriculture and food sectors and build a strategic partnership to address food security.

"Since February the world has witnessed Russia's unjustified invasion of Ukraine and the disruption it is causing to agricultural production, trade, and most importantly, food security," said Secretary Vilsack. "Russia's actions are posing major threats not only to the people of Ukraine but to countries in Africa and the Middle East that rely on the grains and other staples produced in Ukraine. Russia is using food as a weapon and a tool of war to threaten the livelihoods of those around the world, and that is something the agriculture community cannot and will not stand for."

How Risk Professionals talk about Risk



DENIAL

Cyber ? – It doesn't apply to me, ask my managers and lines of business !

ANGER

It isn’t fair – we’re trying to grow a business and create jobs here. Back off with your cyber nonsense !

BARGAINING

I’ll do some of it – it’ll be sort of compliance “a la carte” just to fend off regulators and governing bodies. That should do the job!

DEPRESSION

I’ll never get there – it’s not just laws & standards, but also documentation, technical investment, ongoing monitoring. I just can’t!

ACCEPTANCE

It’ll be okay! – it’s not rocket science, we’re doing a good bit already and we can now bridge the gap and stay ahead !

PHYSICAL SECURITY

- Access to building
- Physical Assets
- IT Hardware
- Vehicle Fleet

Operations Manager, Security Staff

PEOPLE SECURITY

- Permanent & Contract Staff
- Partners
- 3rd Part Employees
- Visitors
- Special Events Security

HR, Security Staff

DATA SECURITY

- Trade Secrets
- Employee Data
- Database
- Customer Data

HR, IT Team & Manager

INFRASTRUCTURE SECURITY

- Networks
- Remote Sites
- Remote Users
- Application Security
- Website
- Intranet

IT Team & Manager

CRISIS MANAGEMENT

- Documentation & Work Procedures
- Emergency Response Plans
- Business Continuity Plans
- Disaster Recovery Plans

Operation Manager, IT Team, HR

5 Pillars of Security Framework™

As a CEO-C-Level-Board Member am I confident/sure/happy that:

1. **All data** including employee data, client data, 3rd party **data is protected appropriately and in compliance with applicable laws & mandatory standards**

2. The organization is able to and does **classify data according to its privacy level**

3. The organization has **put in place appropriate technical security solutions** and/or security measures to **protect data we create, acquire, store, transmit and also dispose of**

4. **If the regulator(s) or enforcement bodies perform an audit I can demonstrate my organization's compliance** (or demonstrable road map to compliance)

5. The organization has **developed and demonstrably deployed security policies and procedures to all staff across the organization** regardless of ranking level, location, business unit or function

C-LEVEL & BOARD MEMBERS EDUCATION

- Face to Face Workshop
- eLearning

5 PILLARS OF SECURITY FRAMEWORK - ASSESSMENT

- Super Strategic
- Strategic

5 PILLARS OF SECURITY FRAMEWORK - SCORE

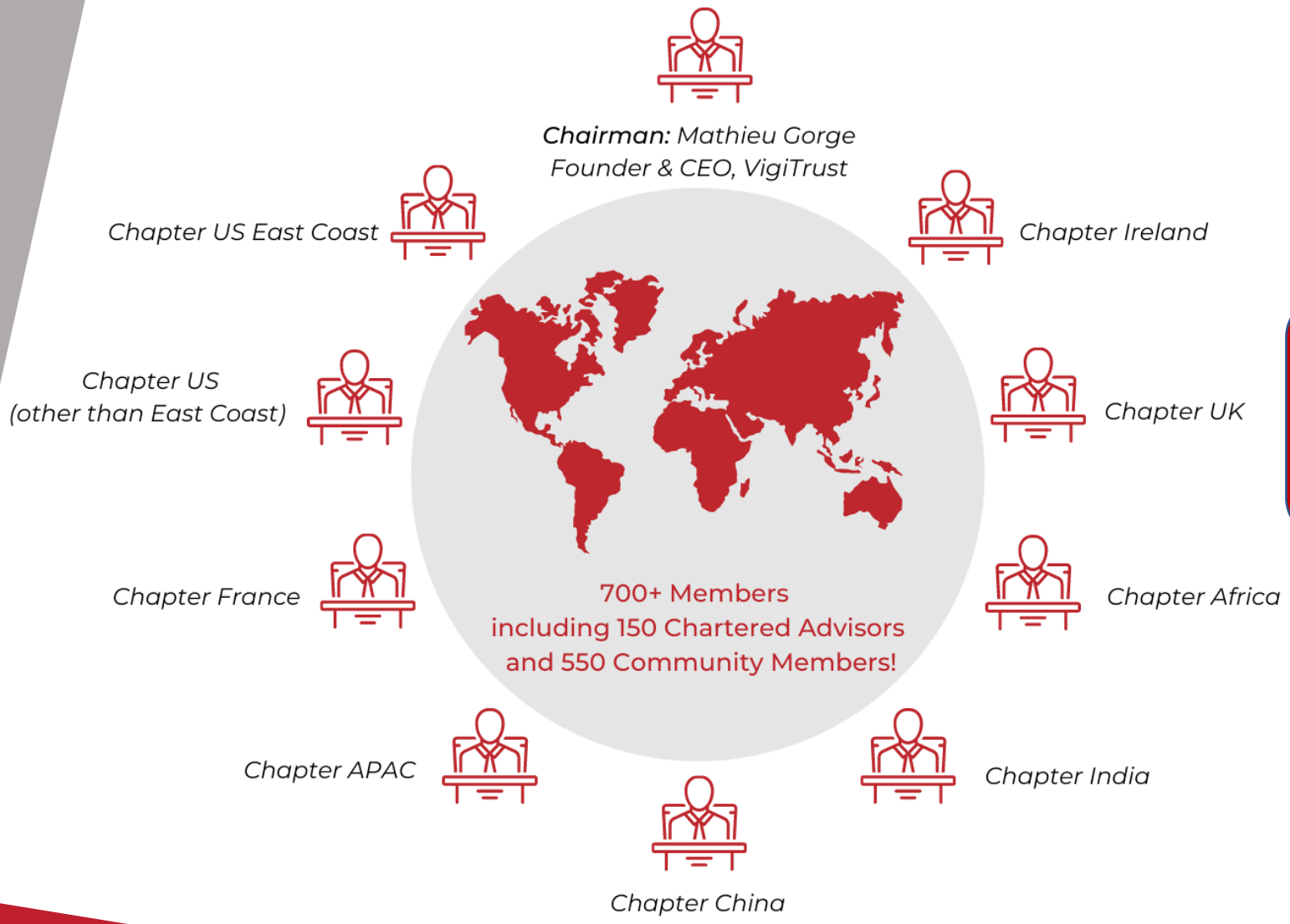
- Action Items
- Red Flags

OPERATIONAL SECURITY, RISK & COMPLIANCE PROGRAM

Empowering CEOs, CxOs, Boards and Senior Security & compliance Pros to talk about Cyber risk and cyber accountability in a collaborative and judgement free way!

Dublin, Ireland, May 10th & 11th 2023
Annual in-person VGAB

Global Leadership Team



Global Leadership Team
25 Subject Matter Experts
Chair
Vice-Chair

The Cyber Elephant in the Boardroom

GUEST CHAPTER CONTRIBUTORS

James Grundvig
Author and Tech Journalist
Breaching the C-Suite (CEOx, CxOs and Boards)

Nina Shulepina
Banking Compliance Professional
Member Of The VigiTrust Global Advisory Board
Protecting Data as the New Currency

Cathy Smith
Founder, Women in Tech NJ & NY
The Intersection of Cybersecurity and Business Digitization

Marco Antonio Soriano
Chief Investment Officer, Soriano Family Office
Handbook for C-Level and Board Members

Bob Gardner
Partner, New World Technology Partners
Managing the Cyber Risk Impact of Capital and Valuation

Nicolas Vigier
CxO Advisor – Cyberstrategy, Coalfire
Cyber Risk Impact on the Board

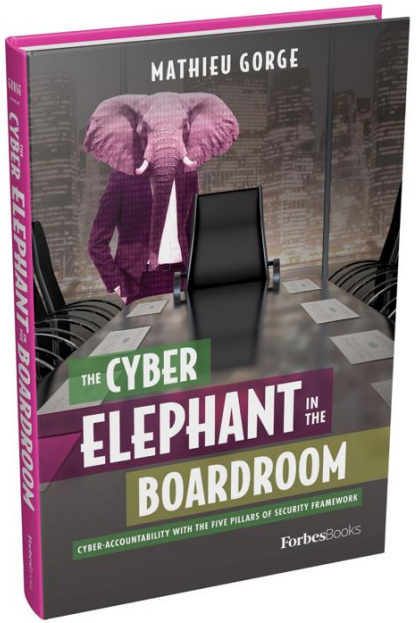
Ed Adams
CEO, Security Innovation
Software – Catalyst for Today's Digital Business

Marie-Christine Vittet
VP Compliance, Accor
To Comply with PCI DSS and keep Cardholder Data Secure

Cecile Martin
Partner, Ogletree Deakins International LLP
Cybersecurity Risk in Human Resources

Thibaud Lexerois
Attorney, Ogletree Deakins International LLP
Cybersecurity Risk in Human Resources

Alexander Abramov
Past President, ISACA New York Metropolitain Chapter
Education for Key Decision Makers



VIGITRUST

Most Influential Business Leaders in CYBER Security 2022

Integrated Risk Management SaaS Provider

Global Privacy Day 2023

mathieu.gorge@vigitrust.com

https://ie.linkedin.com/in/mgorge

CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

> Les outils de la conformité

Les outils de la conformité

Le RGPD offre une boîte à outils diversifiée pour permettre aux organismes de gérer leur conformité d'une façon dynamique et de démontrer qu'ils respectent la règlementation : registre des traitements, mentions d'information, analyses d'impact sur la protection des données, encadrement des transferts, référentiels, certifications ou codes de bonne conduite.

Le registre des activités de traitement

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles.

> Comment élaborer son registre ?

Les exemples de mentions d'information

Pour vous aider à informer les personnes dans des conditions conformes au RGPD, voici quelques exemples pratiques de mentions d'information.

> Utiliser les modèles

Les cadres de référence

La CNIL élabore des cadres de référence permettant de guider les organismes dans la mise en conformité de leur traitement.

> Les cadres de référence

L'analyse d'impact relative à la protection des données (AIPD)

Une méthode et des catalogues de bonnes pratiques, un logiciel open source permettant de réaliser une analyse d'impact relative à la protection des données (AIPD).

CNIL.

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

Le code de conduite

Les codes de conduites sont l'un des nouveaux outils de conformité prévus par le RGPD. Ils permettent une harmonisation des pratiques au niveau d'un secteur d'activité.

Ce qu'il faut savoir sur le code de conduite

Un code de conduite est un outil de conformité sectoriel qui permet de répondre aux besoins opérationnels des professionnels concernés dans leurs démarches de mise en conformité au RGPD.

Que doit contenir un code de conduite ?

Le contenu d'un code de conduite est encadré par le RGPD et par des lignes directrices adoptées par Comité européen à la protection des données (CEPD) qui fournissent des explications et exemples pratiques.

L'organisme de contrôle désigné par le code de conduite

La bonne application d'un code de conduite par ses adhérents fait l'objet de vérifications régulières. La CNIL rappelle le rôle et les obligations de l'organisme de contrôle.

Comment faire approuver un code de conduite ?

Les projets de codes nationaux sont examinés et approuvés par la CNIL alors que les projets de codes européens sont soumis à l'avis du Comité européen à la protection des données (CEPD).

Are we actually moving forward?

VIGITRUST

Pro-active Enterprise Security

What's new in Security in 2007?

- Compliance still very high on the agenda
- Business Continuity Issues
  - 5+ years since 9/11
  - Focus on natural disasters
- Identity Theft & Phishing scams
  - Affecting online transactions such as online banking
  - Still very effective for attackers
  - Based on Spam attacks – many organizations still not prepared against such basic threats
- Number of Defaced Websites in 2006 & 2007 is increasing by the day
  - Estonia vs Russia
- Mobile Phone & PDA Security
- Virtualization
- Wireless Threats
- Data Leakage
  - Veterans in the US
  - Unclaimed laptops auctioned in Heathrow airports
  - Printed information also leaked