VIGITRUST

Integrated Risk Management SaaS Provider

Global Advisory Board

La Cyber Responsabilité en 2021

mathieu.gorge@vigitrust.com

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

IRM Expertise

Featured ForbesBooks AUTHOR

FINANCE MONTHLY GAME CHANGERS AWARDS 2019

CEO TODAY GLOBAL AWARDS 2019

AI acquisition international Cyber Security awards

VigiTrust - the Republic of Ireland

Best Information Security Compliance Management Platform 2020

The Cyber Elephant in the Boardroom

Published by ForbesBooks
November 24th 2020

Available on Amazon, Nook and Apple

LAWYER INTERNATIONAL LEGAL 100 2021 WINNER
MATHIEU GORGE
VIGITRUST
Best IT Security & Risk Management Business Leader - USA

Advisory Board

VIGITRUST

Key Speakers of the Advisory Board


Mathieu Gorge
VigiTrust
CEO & Global Advisory Board Chairman


Marie Christine Vittet
Accor
VP Compliance


Paul Rodgers
Vendorcom
Chairman


Brian Pennington
Coalfire
Regional Sales Director - ROW


Gabriel Leperlier
Verizon
Senior Manager Security Consulting EMEA


Patrick Agopian
Groupe Credit Agricole
Chief Risk Officer


Christopher Moks
Deloitte
Director/Forensic


Karl Bommé
Iceberg Projets
Fondateur


Cecile Martin
Ogletree Deakins
Managing Partner


Bob Gardner
New World Technology Partners
Founding member


Rowan Fogarty
VigiTrust
COO


Ian Pemberton
Interpol
Criminal Intelligence Officer, Financial Crimes Unit


Ed Adams
Security Innovation
CEO & President


Sharon Claffey Kaliouby
Learning Pool
VP North America


Simon Russel
Bronzeye
Managing Partner


Jean Christophe Marten Perolin
French Ministry of Interior
French National Police senior liaison officer in New York City


Philip Mills
Queen's University Belfast
Head of Business Development


John Davies
Pervade Software
Director

Members of the Advisory Board

- Accor
- Alabama District Attorneys Association
- AML Factory
- Aon
- ATHENA
- Avocado System
- Bronzeye
- Coalfire
- Cohen Partners
- Credit Agricole
- Deloitte
- Edgesys
- Iceberg Projets
- ICT Skillnet
- Interpol
- ISACA New York Metro
- JP Morgan
- Learning Pool
- Lewis Silkin
- Lockdown Risk
- LogMeIn
- Innovation Value Institute
- McElroy, Deutsch, Mulvaney & Carpenter
- Motherboard Group
- New World Technology Partners
- Ogletree Deakins
- Pervade Software
- Queen's University Belfast
- RiskGovern
- Riskskill
- Security Innovation

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

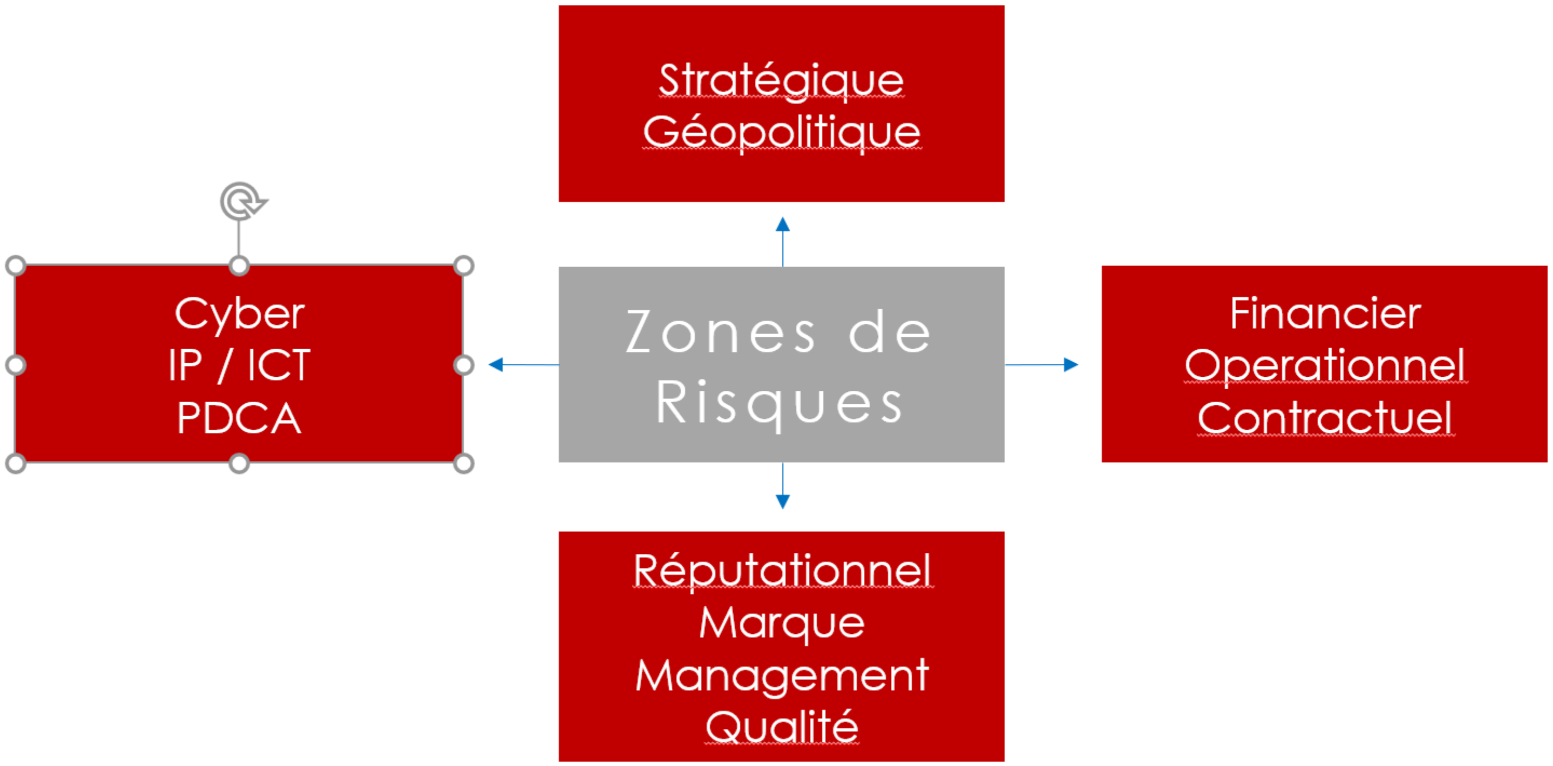
Marie-Christine Vittet
VP Compliance, Accor
To Comply with PCI DSS and keep Cardholder Data Secure

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

Paysage Global des risques



DBIR Review

Incident vs breach

We talk a lot about incidents and breaches and we use the following definitions:

Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

Figure 2. What tactics are utilized? (Actions)

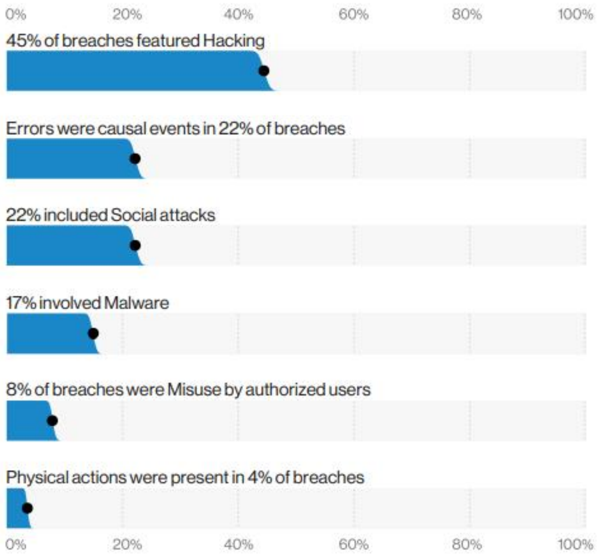
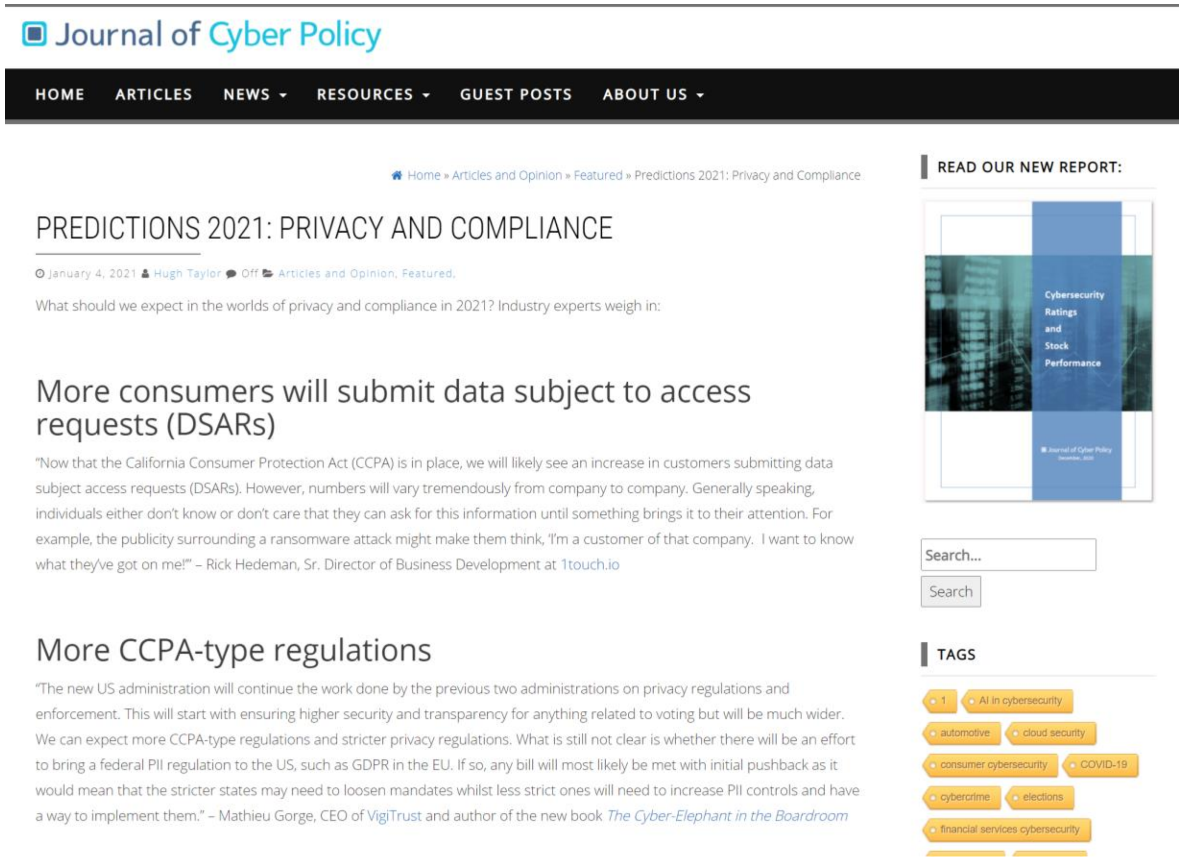


Figure 13. Top threat Action varieties in breaches (n = 2,907)

Predictions

- More of the same, read my 2020 Predictions ☺
- Phishing attacks will keep rising
- More ransomware attacks
- More sophisticated CEO – C-Suite attacks
- Attacks will get personal
    - Social Media
    - Personal Home Infrastructure
- Attacks on Critical Infrastructure
    - Health Systems
    - Banking
    - Transportation systems
- Compliance audits will be more frequent
- More GDPR fines
- More CCPA type regs on the way in the US
- More GDPR type regs worldwide
- Brexit Issues related to Data Protection

- Other than that…nothing to worry about ☺



February 8, 2021

Coping with phishing scams around COVID-19 vaccines and other impending attacks

Mathieu Gorge

Today's columnist, Mathieu Gorge of VigiTrust, expects attacks to emerge around any new COVID-based legislation passed by the Biden administration. He offers some strategies for managing the continued escalation of cyberattacks. BidenForPresident CreativeCommons Credit: CC BY-NC-SA 2.0

While a vaccine for COVID-19 has been rolled out over the past several weeks, distribution has gone very slow. After being stuck at home for almost a year, people have lockdown fatigue and need faster solutions and a sense of hope.

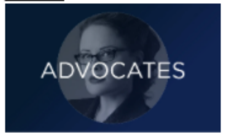
Hackers will view this fatigue as yet another major opportunity to strike. As vaccines are made available, the security industry expects a wide number of phishing scams to surface that lure people into buying "early releases" of vaccines from Pfizer and Moderna. I fully expect the emails to include very realistic logos for those firms, a special discount if the victim buys immediately, and a link to register and pay online that requires not only credit card info, but also some very sensitive protected health information.

Similarly, as President Biden tries to roll out COVID-19 relief, we expect to see scams around any new programs the new administration enacts. Expect bad threat actors to spread ransomware and other threats that will encrypt or destroy data on machines.

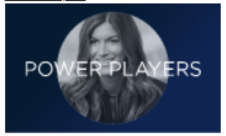
On top of that, the threat landscape has kept expanding with new strains of ransomware discovered late last year and the devastating Solar Winds supply chain hack. Throughout the COVID-19 period, security professionals have noticed a huge increase in cyberattacks on companies, governments, and individuals on four key fronts: operations, technology, data, and legal aspects of security. Here's some advice on how best to manage these trends:

- **Operations:** Many companies had no choice but to ask their staff to work from home. Some already had some staff travelling or working from home and could just extend the policies, procedures, and training for secure telecommuting to a wider population. Others were completely unprepared and just asked their staff to work from home devices to access company systems and data, simply because they did not have any plan. Either way, on a global basis, the overall attack surface available to hackers and criminals just increased exponentially, nearly overnight overnight.
- **Technology**: As companies started to realize the risk was real and started addressing it with technical solutions, policies, and training for secure WFH, the bad guys were already at work spreading malware, phishing and attacks on extended networks, data storage, and remote access to systems.
- **Data**: Organizations are urged to investigate data usage – specifically, which applications and what data should be made available and to whom? Is there a data classification and associated systems access policy, ideally including multi-factor requirements? Is the organization offering clear guidance on how to manage the crossover between private and personal life on private and corporate devices?

Women in IT Security honorees: Advocates

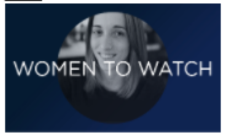


Women in IT Security honorees: Power Players



Women in IT Security honorees: Cyber Veterans

Women in IT Security: Women to Watch



MOST POPULAR

Popular | Emailed | Recent

SentinelOne forks over $155 million for log management company

Google Firebase hosts Microsoft Office phishing attack

Google pitches security standards for 'critical' open-source projects

A water-treatment hacking, and the complexities of risk mitigation

Pensacola incentive campaign portrays a paradise for remote cyber workers

TECH

What you need to know about the FireEye hack: Cybersecurity attack against US government

Nathan Bomey and Kevin Johnson USA TODAY
Published 2:08 p.m. ET Dec. 14, 2020 | Updated 6:59 a.m. ET Dec. 18, 2020

This Wednesday, Feb. 11, 2015 photo shows FireEye offices in Milpitas, Calif. The cybersecurity firm said Tuesday, Dec. 8, 2020 it was hacked by what it believes was a national government. The attacker targeted and stole assessment tools that FireEye uses to test its customers' security and which mimic the methods used by hackers, the company said. *Ben Margot, AP*

But the full extent of the damage is not yet clear.

"Think of it like a health virus that manages to get into your body," said Mathieu Gorge, a cybersecurity expert and author of the forthcoming book "The Cyber Elephant in the Boardroom." "Once it's in your body, it multiplies, using all of the organs and all of the arteries and all the liquids in your body. Everything is interconnected."

Here's what you need to know so far.

What information was potentially taken?

It's too early to say since the attack was only recently discovered but appears to have exploited what SolarWinds called a "potential vulnerability" related to updates released between March and June for Orion, which helps monitor networks for problems.

But early indications suggest the attackers were seeking information on American hacking capabilities and defenses. Call it the latest phase in what could be a cyber-era cold war.

"It appears the attackers may have taken our own tools for finding vulnerabilities in foreign networks," said Matthew Schmidt, a professor in the national security department of the University of New Haven's Henry C. Lee College of Criminal Justice and Forensic Sciences. "They hacked our hacking capability. It's very early, but the level of immediate reaction suggests a very, very serious intrusion."

GUEST INTERVIEW

MATHIEU GORGE, CEO, VIGITRUST

Gorge discusses the impact of Brexit on gaming firms and GDPR, something he describes as a topic containing many "unknowns"

VigiTrust is currently being kept busy with impending GDPR changes amid Brexit, with the UK's decision to leave the EU set to have a major impact on data transfer.

The Integrated Risk Management SaaS solutions provider allows clients to maintain compliance with legal and industry regulations on data privacy and information governance.

As such, VigiTrust CEO Mathieu Gorge spoke exclusively to *Gambling Insider* about how gaming companies can remain compliant amid changes in GDPR.

"I would say there is a portion of companies that are compliant," explained Gorge. "Then you have a section of the market where they're not in compliance but they're in the process of being compliant. They might be 60% or 70% compliant – because they do have good technology, they have encryption, they do training, they have policies, they regularly try and benchmark themselves – but they're not fully compliant.

"Then there's a portion of the market that's just starting out. And of course there's a portion of the market where – especially for smaller businesses – it's not that they're paying lip service to it, but they're saying 'until somebody knocks at the door, it's not really my problem'.

"And that's the wrong thing to do because you could be a small business and still have very sensitive data."

VigiTrust has helped companies across various industries remain compliant with data regulations, and Gorge offers advice on how those within the UK gambling industry can remain on the right side of the law post-Brexit.

"The advice to companies will be to just assume they need to comply with – at the very least – the requirements of GDPR, and that they need to have people who are held accountable within their organisation," added Gorge.

"You find that concept of accountability at the very beginning of GDPR, where it basically says the company needs to be accountable for data protection.

"If I was on the board of a UK company right now, and I was talking about cyber security, I would want my CCO, my chief legal officer, to talk to me about that very question about data transfer. I would want this to be a broad matter because of the unknowns. It could be nothing, or it could be that it leads to a fine, it leads to our company name in the media and so on, and we want to avoid that.

"There have been big fines like Marriott and British Airways, and some small fines are currently being issued by the French regulator, CNIL. There were a few fines at the beginning of the year in the region of £7,000 ($9,500), £10,000 and £15,000 for smaller organisations.

"I think what they were trying to do was to make a point that if you're a smaller organisation but you're doing something drastically wrong, you're still going to be fined; it's still going to be a pain, and your name is going to be published."

"The advice to companies will be to just assume they need to comply with – at the very least – the requirements of GDPR, and that they need to have people who are held accountable within their organisation"

Often times, threat actors will use the Dark Web to find people to work with. In one post, someone is looking for a person with experience in "CEO fraud." In another, an insider at a Spanish bank asks to be pinged on Telegram, a cloud-based instant messaging service.

Going after a CEO also has advantages, according to Sixgill, because an imitated email from the top means people will often click on it or respond quickly and reflexively.

A threat actor looks for someone to work with who has experience in CEO fraud. (Sixgill)

Les Entreprises Françaises sont aussi ciblées

Le Monde

Consulter le journal

ACTUALITÉS | ÉCONOMIE | VIDÉOS | OPINIONS | CULTURE | M LE MAG

PIXELS • SÉCURITÉ INFORMATIQUE

Partage

Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs

Le centre hospitalier, qui compte près de 2 500 lits d'accueil, se remet progressivement de la paralysie informatique provoquée par un virus de type rançongiciel.

Teller Report

Now you can see non-English news...

ENHANCED BY Google

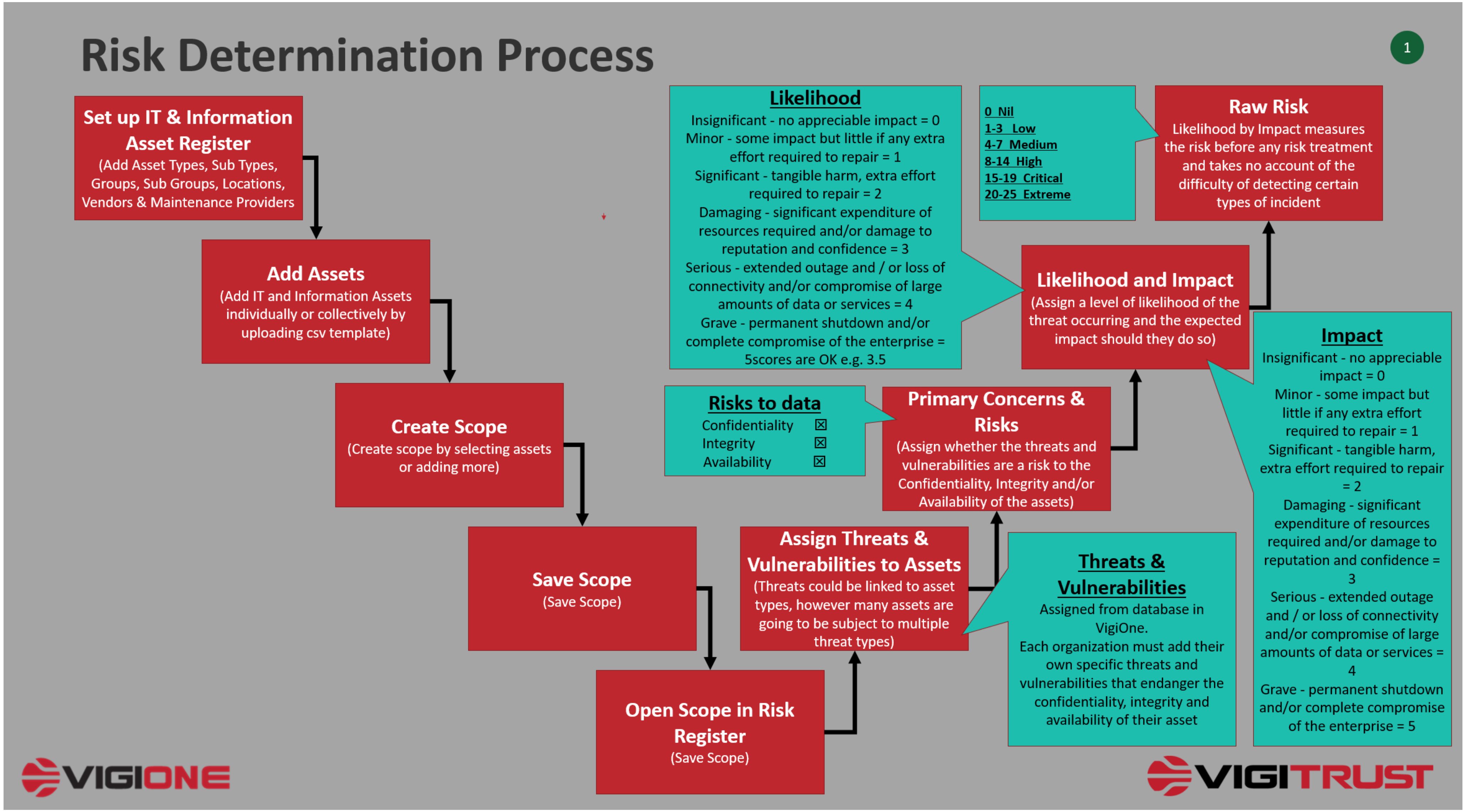
Home | News | Business | Sports | Life | Tech

Bouygues still affected by a cyber attack launched on Thursday - France 24

2/5/2020, 6:31:16 PM

Bouygues still affected by a cyber attack launched on Thursday

How Risk Professionals talk about Risk



How do CEOs, CxOs, Boards talk about Cyber risk and cyber accoutability

Cyber Accountability – PCI DSS Viewpoint

Table 1. Common PCI DSS Roles and Responsibilities

Roles and Teams	Examples of PCI DSS Responsibilities
Executive Sponsors, Leader, Owner	• Authority to provide direction and budget. • Accountable for the risk and/or delivery of PCI DSS compliance.
Compliance Managers	Manages ongoing compliance efforts and the completion of PCI DSS validation documents such as Attestations of Compliance and Self-Assessment.
Information Security Team	Responsible for the security controls applied across the business. This includes overall accountability for: • Information security • Policy • Acceptable-use guidelines • Awareness • Incident response
Business Unit Managers	• Ensures business unit payment card controls are enforced. • Assists in removing payment card information from processes. • Helps make processes compliant.
Audit, Risk Management Team	Guides risk assessment and governance responsibilities.
Information Technology Team	The staff or outsourced third party providing and operating the organization's computer network(s). IT Administrator/s are vital to identify due to their span of responsibility.
Third-Party Service Providers	Outsourced processes, technology, staffing, or purchased PCI DSS solutions.
All Staff (Organization)	Understanding of their responsibilities to protect cardholder data.
QSAs/ISAs	Subject-matter experts in PCI DSS compliance.

Accountability

Compliance/Governance

Cyber Accountability – GDPR

Accountability obligation

Accountability is a common principle for organisations across many disciplines; the principle embodies that organisations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with. The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested.

Organisations, and not data protection authorities, must demonstrate that they are compliant with the law. Such measures include:

- Adequate documentation on what personal data is processed;
- How, to what purpose, and how long data will be processed for;
- Documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; and
- The presence of a Data Protection Officer (if required) who is integrated in the organisation planning and operations etc.

Make an inventory of all personal data you hold and examine it under the following headings:

- Why are you holding it?
- How did you obtain it?
- Why was it originally gathered?
- How long will you retain it?
- How secure is it, both in terms of encryption and accessibility?
- Do you ever share it with third parties and on what basis might you do so?

This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business. The inventory will also enable organisations to amend incorrect data or track third-party disclosures in the future, which is something that they may be required to do.

You should also reference our guidance on Data Protection Officers, Data Protection Impact Assessments and the Risk-based Approach to processing activities to see whether any of the criteria laid down there are of relevance to your processing activities.

Source:

An Coimisiún um Chosaint Sonraí
Data Protection Commission

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

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

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

Integrated Risk Management SaaS Provider

Global Advisory Board

La Cyber Responsabilité en 2021

mathieu.gorge@vigitrust.com

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

VigiTrust - the Republic of Ireland
Best Information Security Compliance Management Platform 2020