

Hello and Welcome!



all right reserved





The Art of Compliance in the Era of Cyberwar

*“The probability of facing a cyber incident is so high it is no longer feasible to exclude **security as strategy** to protect critical digital systems and **guarantee cyber resilience**.”*

Regulation is often perceived as a cost.

*However, this session aims to illuminate how your business can **optimize regulation as a competitive tool** all while **future-proofing** your business. “*

European Central Bank Shuts Down 'BIRD Portal' After Getting Hacked

Good to know....

- Compromised in December but *discovered* in August
- Discovery happened during a maintenance check-up
- Only statements about *personal data* that was affected, nothing about company data
- Nor any specific statements about how this incident could affect the entire B2B chain

9-month window between being compromised and detection!

Could your business survive?

Top 3 FinTech Security Breaches Alongside Redtail

The FinTech market has extremely high requirements in regard to increased innovation and enhanced features. Thus, FinTechs can lose focus on security and endanger their clients' data. Could Redtail, Fiserv, Voya, and BlackRock have prevented their data issues? What should these companies do to restore their security levels and forestall a relapse?

Fintechs are not immune to the risks involved in cyber!

- **RedTail > bad data management + public accessibility**
- **Fiserv > authentication loophole**
- **BlackRock > human error**

Agenda

1. The Risk Society
2. The business case of security as strategy
3. Legacy thinking
4. So what's your security strategy?
5. What can you do TODAY to do it better?
6. How can we help you do that?

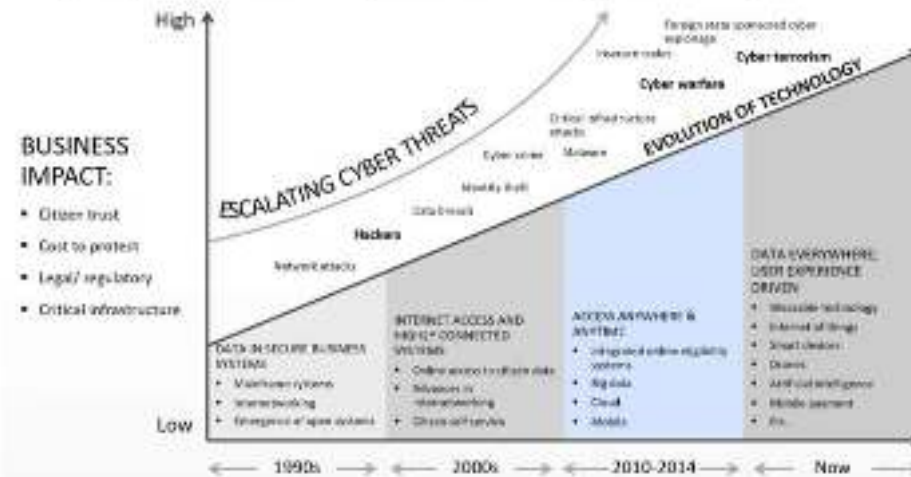
The Risk Society – The Realities for Digital Businesses

- The Risk Society: the type of risk emerges from the **ubiquitous and embedded nature of technology**
- The more your core business is digital, the higher the threat of these risks

CONCLUSION...

THREATS

Complexity of Cyber Attack Capabilities are Growing (2014 Survey)



... you have an organic interest in becoming cyber resilient.

The Business Case of Security as Strategy

Security from a business perspective – eliminating friction

- Globalization is passé, we are now **so interconnected** that any compromise in the chain can have huge consequences!
- Such incidents have led to a **bottom-up approach** so entities are secure, but when they are compromised, the community can respond e.g. intelligence sharing in the US banking sector

you CANNOT afford to be the weak link in the chain, no matter your size!

You feature in the risk register of your consumers

AND business partners!

So ... security as a strategy means *optimizing* your security according to your business needs but it also means being informed and knowing how to act.

Some Security Options ...How to choose?

The image displays a comprehensive grid of security vendor logos, organized into several key categories:

- Network & Infrastructure Security:** Includes vendors like Palo Alto Networks, Fortinet, Cisco, and SonicWall.
- Web Security:** Features companies such as Cloudflare, Akamai, and Imperva.
- Endpoint Security:** Lists vendors like Symantec, McAfee, and Trend Micro.
- Application Security:** Includes SAST and DAST tools from vendors like Veracode and Checkmarx.
- Cloud Security:** Features CSPM and CASB solutions from vendors like Palo Alto Networks and Microsoft.
- Mobile Security:** Lists vendors like Symantec and McAfee.
- Identity & Access Management:** Includes Okta, Microsoft Entra ID, and Ping Identity.
- Security Ops & Incident Response:** Lists Splunk, Palo Alto Networks, and IBM.
- Threat Intelligence:** Features Anomali and Recorded Future.
- IoT Security:** Lists vendors like Cisco and Palo Alto Networks.
- Supply Chain Security:** Includes vendors like OpenText and SAP.
- Other categories:** Includes Risk & Compliance, Data Security, and Mobile Security.

The Business Case of Security as Strategy

Security from a regulatory perspective – national interest

- The regulator is also worried....and responding!
- We see a trend where the security interests of private companies are being elevated to a level of national security interest, this in tandem with the rising digitalization of society
- Characterizing the regulator from a business perspective:
 - Hyperregulation
 - Monolithic laws vs diverse market ecosystems
 - Logical/technical deficits

Conclusion: legal uncertainty and inequitable situations



The Bottom Line...

from a business *perspective*,
regulation is at best a hazard



and at worst a huge cost, all
while Rome appears to be
burning!

Let's change that, shall we?



Is a knife...

**Le véritable voyage de découverte
consiste non pas à chercher de
nouveaux paysages, mais à avoir de
nouveaux yeux. - Proust**

unity in the same year
for regulation!

So what's your security strategy?

Your security strategy?



The Network and Information Security Directive (NIS)

Just briefly....

- What > Networks and Information Security
- Scope > Essential Service Providers determined by
 - The effect you will have if you have an incident
 - The authorized governmental supervisor

What we're really seeing here is:

1. The security of *private companies* is now a *public good*
2. The regulator has the power to decide that you are essential, even if you don't meet the exact legal requirements
3. The regulator is *fostering a cyber community* lead by the Center for Cyber Security (CCB)
4. This is a *continuum* of the Single Digital Market strategy of the EU

The particularity of the NIS is that it DOES NOT come with heavy penalties....

From the Art of War...

...to the Art of Compliance

Know yourself
Know your Business

Know your enemy
Understand the threat
landscape and actors

Know your terrain
Understand your
environment

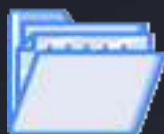
Assets



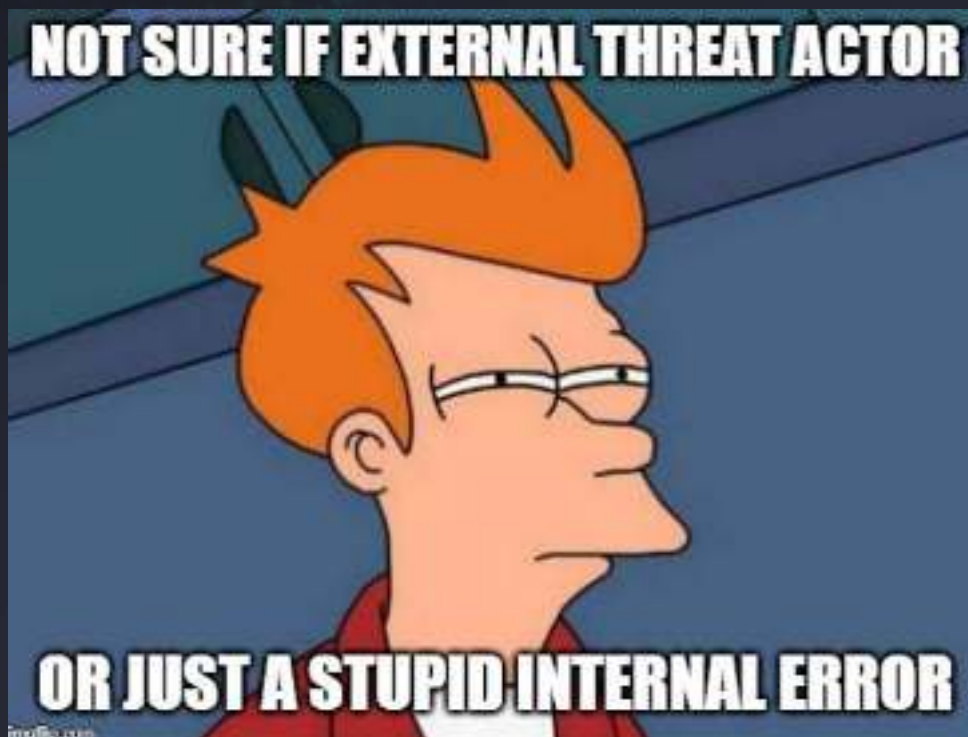
Operations



Objectives



Strategy



Interconnected
financial world



Stakeholders



The Consumer



The Regulator


The Art of Compliance – Leverage the Regulator and don't do a hack job!

Security from a strategic perspective – optimization through orchestration and integration

- ISO 27K is an internationally recognized standard, now being favoured by the EU as *the* tool to implement a **security strategy from A-Z**
- The regulator is making it clear that there needs to be a **cyber community with a united vision** so using the same guideline makes sense
- It's not just about *your* security but **about the entire financial ecosystem**, so speaking the same “language” is helpful

The EU has a Single Digital Market strategy, so compliance to one regulation builds on the last!

So be smart and build on what you already have done, and make sure you future-proof yourself by not creating legacy or friction from day one!



**What can
you do
TODAY to
do it better?**

Thank you for your time!



**Inspiring
the cyber security
community**

APPROACH COMPANY PRESENTATION
THE 11TH OF SEPTEMBER 2019



In case you'd like to reach out...

Giselle van Tornout from Approach Belgium



Mob: +32 472 90 23 69

giselle.vantornout@approach.be