The Security Transformation Research Foundation

Cyber Security: Not just an Equation between Risk Appetite, Compliance and Costs

Cyber security is becoming a matter of good corporate governance, good ethics, and quite simply – good business.

Key factors for boards and executive management to consider in 2019

January 2019

Cyber security is now recognized as a key concern at the top … but how deep is the Board commitment ?

Cyber security has risen as a key issue on the radar of virtually all organizations.

Cyber attacks have been topping executives' lists of business risks for three straight years (AT Kearney, 2018, among many others!) (*)

3 main drivers:

- Non-stop cyber attacks and a cyber risk landscape which is ever-complexifying (and emerging new technologies, e.g. driven by AI, which will become double-edged swords).
- Security and privacy become increasingly visible to and valued by customers.
- Regulators have stepped firmly into the topic (GDPR in Europe, California Consumer Privacy Act 2018).

Yet there is still a significant discrepancy between the salience of the issue at Board level and the actual steps taken to address it

An overwhelming majority of organizations have experienced cyber attacks.

Yet 60% of surveyed organisations have not yet fully developed and implemented a cyber defence strategy (AT Kearney, 2018) (*).

More than under-investment, the situation is rooted in 15 years of business-driven adverse prioritization around the execution of protective security measures:

- Leading to the failure to deliver adequate protection and adherence to security good practices in many large firms
- Also leading to a significant talent alienation problem around cyber security, which is making the situation self-perpetuating

What will it take to move the lines ? (for good)

(*) https://www.atkearney.com/web/global-business-policy-council/article?/a/rising-to-the-challenge_2018

Cyber security cannot be left to the CIO or the CISO to deal with

The "**WHEN-NOT-IF**" paradigm around cyber attacks has changed the deal completely around cyber security

- Cyber security can no longer be seen just as an equation between risk appetite, compliance requirements and costs
  - Cyber attacks WILL happen
  - Sooner or later, regulators WILL step in
  - They can now impose BUSINESS-THREATENING fines around the mishandling of personal data
  - Media interest has never been higher around those matters: Business reputation and trust in a brand WILL be damaged by high-profile incidents

The "WHEN-NOT-IF" paradigm turns cyber security into a matter of good corporate governance, good ethics, and quite simply – *good business.*

The Board is ultimately accountable for cyber resilience

Principles of due care and diligence – central to most corporate legislations and regulations around the world – require that relevant skills are represented at Board and executive management level to understand and address matters related to cyber risk

Responsibilities can be delegated, but prioritizing against – or ignoring – cyber security matters at Board level is now bordering on negligence and senior executives could lose their jobs over it

Cyber security must become a building block of the Board's agenda, not an occasional item invited to appear after an incident or as a box-checking exercise

Cyber security is the foundation of digital trust

Digital trust is the bedrock of the digital transformation and is becoming an organization's most valuable asset

- Consumers are increasingly wary of security and privacy issues, and are starting to react to data breaches
- Significant amounts of the value created by organizations' digital transformations could essentially vanish overnight if not properly protected

There cannot be any lasting digital transformation without a strong cyber security practice in place across the enterprise

- This is a matter of corporate culture and governance, as much as technology

Framing cyber security as a key ESG topic

Cyber security must be driven top-down from the Board as an integral part of a firm's strategy

- Protecting personal data and privacy is fast becoming a matter of **corporate social responsibility** for most firms, as consumers and citizens become more and more sensitive to these issues.
- A strong cyber security practice becomes a matter of corporate values, as a fundamental pillar of a sound data protection practice.
- Cyber security must become a key pillar of a firm's **ESG** (Environmental, Social and Governance) practice, as beyond regulatory compliance, avoidance of fines and competitive advantage (all aspects it will support in the short term), a strong cyber security practice also cements longer-term valuations and growth, like many other ESG parameters.

Good cyber security brings value

Data models are starting to back this up.

- In their **Total Societal Impact** study (A New Lens for Strategy, 2018) (*), BCG identify cyber security as a key ESG topic for several industries:
  - Retail and Business Banking
  - Technology
- For those industries, quantitative analysis revealed a **concrete link** between performance on cyber security and both valuation multiples and margins.
- In fact, the same logic could apply to most industries in varying degree**.**
- Strictly, this is not new: We highlighted the mechanics between security, privacy and value destruction in a 2015 white paper (**), and McKinsey & Co before us in a white paper for the World Economic Forum in 2014 (***)

(*) https://www.bcg.com/publications/2017/total-societal-impact-new-lens-strategy.aspx
(**) https://corixpartners.com/wp-content/uploads/2015/01/Corix-Privacy-in-IoT-BigData-Cloud-2015.pdf
(***) http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

The social dimension of cyber security

The whole enterprise is fast becoming data-driven, and with that come new social responsibilities

- Data is being collected on a larger and larger scale, not only about clients but also business partners and employees; a vast proportion of it is personal in nature.
- Decision-making at many levels across the enterprise up to the Board is increasingly data driven.
- Cyber security is at the heart of data protection and is deeply intertwined with some of the most important social issues of our time:
  - The Protection of the **Privacy** of Consumers and Citizens, who are increasingly aware of these matters
  - **Corporate Social Responsibility**, as firms (brands) are increasingly judged by how well they protect their consumers' and employees' data ; breaches can make lasting reputational damages therefore developing and maintaining **digital trust** is paramount.
- Historical business models built around ruthless data monetization are being exposed and may be coming under pressure.

The social dimension of cyber security

Evolutions of data-driven business models towards a greater empowerment of the consumer could make the cyber security issue even more salient

- As privacy concerns by customers and policymakers are on the rise, some are calling for different **data ownership** schemes.
  - Can firms who almost exclusively make money packaging and selling their user's data continue to strive in an age where people become increasingly wary of such practices ?
  - For how long can pointless "click-thru" agreements (hiding tens of pages of extortionate legal content) continue to prevail ?
- Tech companies could end up having to pay users (somehow) for the use of their data.
- Regardless of whether data-driven business models evolve, **data will always need to be protected** (and perhaps even more so if the understanding becomes that organizations do not own the personal data they collect).
- Securing payments and data integrity would be key in implementing such schemes.
- Blockchain technology may play a role in this if it can scale up, but its energy consumption is already raising concerns (*) and this could in turn become a matter for Responsible Investors.

(*) https://futurism.com/hidden-cost-bitcoin-our-environment

Cyber security and corporate governance

A total shift in governance paradigm around data is required, as regulators and legislators step into the topic and societal expectations evolve

- **You cannot do what you want with data (anymore!)**
- Data governance, data management and data protection become key practices in the context of the data-driven enterprise
- Cyber security considerations – as a key pillar of data protection – must start to underpin daily business operations and decisions, and be embedded in the way every firm works
- This has to come from the Board down, as we started to point out in 2015 (*)
- A good cyber security governance framework is essential to the successful delivery of the measures required to adequately protect data

(*) https://corixpartners.com/wp-content/uploads/2015/01/Corix-Privacy-in-IoT-BigData-Cloud-2015.pdf

Cyber security and corporate governance

Execution is key around cyber security: The problem is not knowing what should be done but actually doing it, and driving priorities accordingly

- The roadblocks which have been preventing the full execution of cyber security programmes in the past are almost always governance and cultural matters which can only be solved by top-down corporate approaches driven from the Board.
- This is not a new issue, and decades have been lost in many large firms because of failures to consistently drive cyber defence plans from the board down over the right timeframes.
- This is not about "throwing more tech" or "more money" at the cyber security problem, but engineering the leadership and management levers to get things done
- These aspects are even more relevant for the many firms engaging now in large scale cyber security transformation programmes in order to "catch up" over short timeframes

Summary of Key Points

The "**WHEN-NOT-IF**" paradigm around cyber attacks has changed the deal completely around cyber security.

- Cyber security can no longer be seen as an equation between risk appetite, compliance requirements and costs.
- The "WHEN-NOT-IF" paradigm turns cyber security into a matter of good corporate governance, good ethics, and quite simply – good business.
- Cyber security must become a building block of the Board's agenda, not an occasional item invited to appear after an incident or as a box-checking exercise.

Digital trust is the bedrock of the digital transformation and cyber security underpins it.

Beyond regulatory compliance, avoidance of fines and competitive advantage, cyber security also cements longer-term valuations and **growth**, like many other Environmental, Social and Governance (ESG) parameters.

Good cyber security brings **value** and data models are starting to back this up.

Cyber security must be driven **top-down from the Board** as an integral part of a firm's strategy and a key pillar of its ESG practice.

- Cyber security is at the heart of data protection and is deeply intertwined with some of the most important social issues of our time.
- And a total shift in governance paradigm around data is required, as regulators and legislators step into the topic and societal expectations evolve.

Governance and culture must take centre-stage around cyber security as the problem isn't knowing what should be done but actually doing it, and driving priorities accordingly from the Board down.

Contact Details and Acknowledgements

Jean-Christophe Gaillard / Vincent Viers
Corix Partners
jcgaillard@corixpartners.com
+44 (0)7733 001 530
www.corixpartners.com

Richard Preece
DA Resilience
richard@daresilience.com
+44 (0)7954 694 391
www.daresilience.com

David Hozé
Wise Partners
david.hoze@wise-partners.fr
+33 (0)6 09 75 63 36
www.wise-partners.fr

Many thanks to our focus group members, contributors and reviewers

Peter Adams, Ishkadon
Hugo Bellamy, Wise Partners
Rupert Brown, Evidology
Tim Chambers, CoolDC
Chris Dilloway, Hakluyt
Stuart Duthie, Qualocity
Chris Eley, ITLab
Cornelia Gomez, PAI Partners

Many thanks to **Dan Warburton, Andrew Pryor** and the CIO WaterCooler platform for their support

THE
Security
Transformation
RESEARCH FOUNDATION

www.securitytransformation.com

@Transform_Sec

The Security Transformation Research Foundation is a dedicated think-tank and research body aimed at approaching Security problems differently and producing innovative and challenging research ideas in the Security, Business Protection, Risk and Controls space

FINAL – 1.0 – January 2019