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

corix partners

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

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 lists of business risks for the last few years

4 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 could eventually become double-edged swords);
- Security and privacy becoming increasingly visible to and valued by customers;
- Regulators stepping in firmly into the topic (GDPR in Europe, California Consumer Privacy Act 2018, etc…);
- Since 2020, the COVID-19 pandemic accentuating the dependence of the global economy on digital services

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

Cyber Security is now Recognized as a Key Concern at the Top … but How Deep is the Board Commitment ?

An overwhelming majority of organizations have experienced cyber attacks.

Yet many have not yet fully developed and implemented a cyber defence strategy and operating model

- 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
- A situation which is now compounded by the COVID-19 crisis, but the focus at board level has been for too long on pure operational and compliance matters around security and privacy, to the detriment of longer-term strategic approaches

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

Cyber Security Cannot Be Left to the CIO or the CISO to Deal With

Bottom-up operationally-driven or compliance-driven approaches have failed

*The "**WHEN-NOT-IF**" paradigm around cyber attacks is now changing the deal completely around cyber security for the Board*

- 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 focus has to shift onto the protection of the business and the actual execution of protective measures

The Board is ultimately accountable for cyber resilience

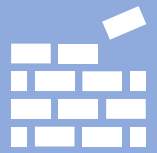
Cyber Security Cannot Be Left to the CIO or the CISO to Deal With

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

- 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

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

Cyber Security is the Foundation of Digital Trust



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

- 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

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

Framing Cyber Security as a Key ESG Topic

Consumers and citizens become more and more sensitive to security and privacy issues.

Protecting personal data and privacy is fast becoming a matter of corporate social responsibility for most firms

- 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.
- 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, and data models are starting to back this up

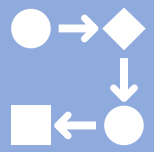
The Social Dimension of Cyber Security & Privacy

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.

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

Good Cyber Security Need Strong 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 must 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 message has to come from the Board down

A good cyber security governance framework is essential to the successful delivery of the measures required to adequately protect data

Execution is Key around Cyber Security

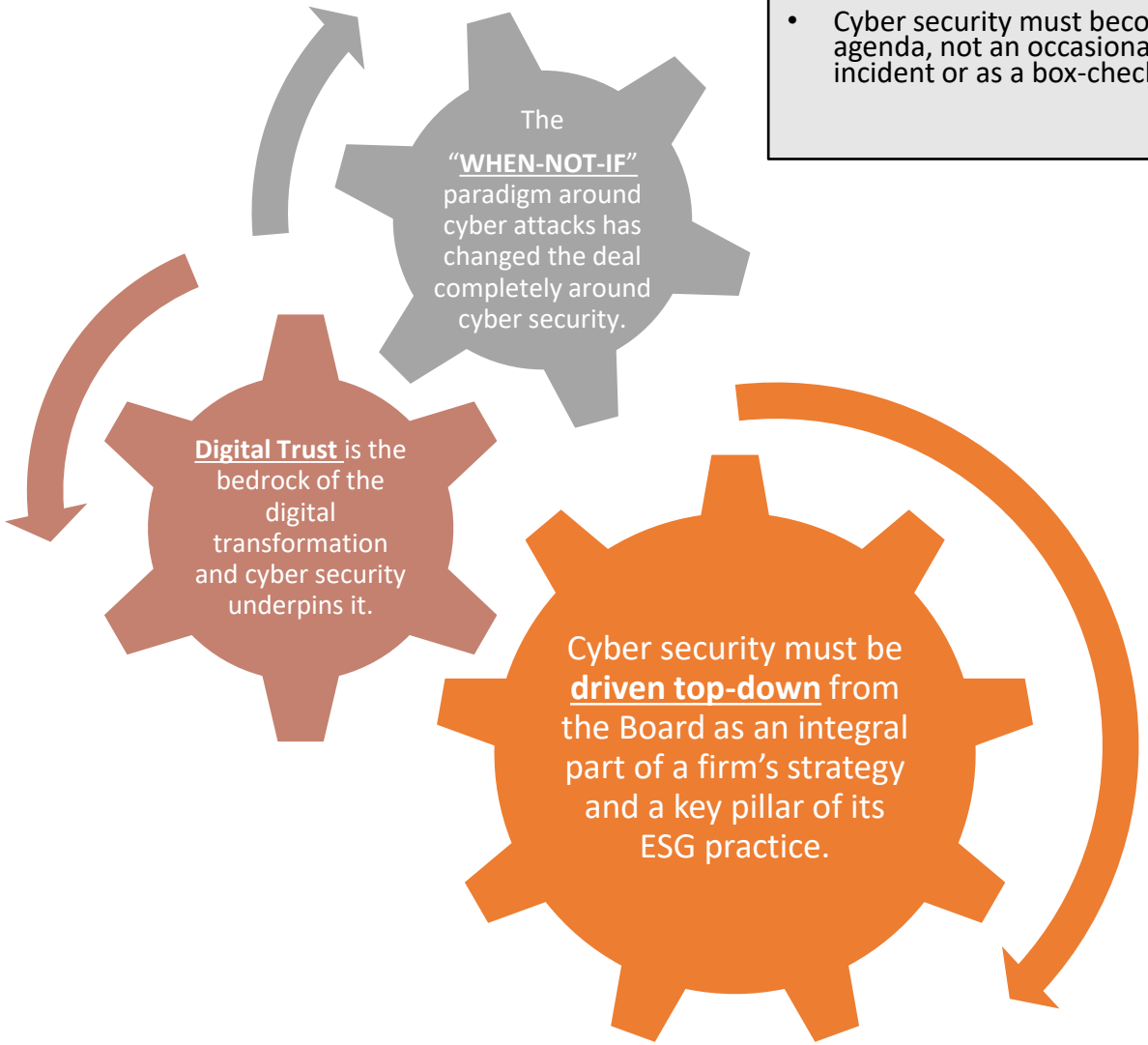
The problem is not knowing what should be done but actually doing it, and driving priorities accordingly

- 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.
- 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

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

Summary of Key Points

- 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.



- 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 is at the heart of data protection and is deeply intertwined with some of the most important social issues of our time.
- 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.

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

269 Farnborough Road
Farnborough, Hampshire
GU14 7LY
United Kingdom

Registered in England and Wales
Corix Partners Limited (No. 06774109)

*Originally published in collaboration with **The Security Transformation Research Foundation** – January 2019*

Please be in touch to discuss further

jcgaillard@corixpartners.com

+44 (0) 7733 001 530

www.corixpartners.com

@Corix_JC

@CorixPartners

Thank You