DISEM INSTITUTE

A solid and sound cyber-security strategy

Validated and future-oriented

https://disem-institute.com/

A solid sound cyber-security strategy, Future-oriented and validated

Society is becoming increasingly dependent on technological developments and digitization, including in the field of cyber-security. This adds to the interconnectivity of society, making it more complex and dynamic. A justified executives' problem arises: "to what extent is the cyber-security strategy future-proof?" and "At what cost is its implementation accepted?" The current past-oriented decision support tools of risk analysis, benchmarks and standards will not provide an answer. Disem Institute has a forward-looking approach that is grounded in the scientific method of dynamic modelling. This approach (1) provides insights into the causal relations of the structure underlying complex problems, (2) shows how a real-life strategy will evolve in the future and (3) provides insights for adjustment and follow-up actions. This way of working gives strategic assurance about the potential success of a cyber-security strategy before it is implemented.

Technological development and digitalisation

Today, we live in an advanced, digital society, wherein technological developments are evident and evolve at a rapid pace. Powerful and fast-advancing networks, more innovative digital devices and advancing automation are visible everywhere. This leads to a noticeable increase in interdependence and connectivity.

These technological developments are increasingly influencing our daily lives through wearables, home appliances connected to apps and fast, and mobile technology. In the 24/7 economy, mobile technologies are used more and more for business as well as private communication. We are constantly available in such society and the urban areas will become fully digitalized through a smart city concept. There is also rapid growth of automated and robotic process technology for companies. Self-thinking, self-reasoning and self-learning software is an unstoppable development.

Consequently, this creates a society that has an improved technological cohesion and is more and more interconnected while rapidly digital innovations are emerging. It is precisely because of this innovation that better communication and thinking power are present and potentially useful in a broader sense. As a result, (adequate, necessary and decisive) activities automatically take place more quickly. This digitization is highly topical and applies to society as a whole. It is precisely and emphatically applicable to the field of cyber-security.

Good and adequately-functioning strategies can be implemented by using a scientifically-validated method of dynamic modelling. Likewise, this method can be applied to analyse complex, dynamic, social issues. By doing so, there are innovative means to support the next generation of strategic management.

> *Complexity and dynamics in digitization lead to a question of insight and understanding for adequate decision-making.*

Strategy, governance and IT

From a strategic point of view, directors of organizations often ask themselves “How much money can be spent on cyber-security?” After all, they can only spend money once. All the budgets allocated to cyber-security cannot be available for other strategic business activities. While the costs for cyber-security are clear, the benefits of avoiding potential future cyber-attacks seem vague and far away.

This means that decision-makers are usually reluctant to invest money in a necessary and adequately-functioning cyber security strategy. By nature, mankind is risk averse and has a preference for certainty. The costs for good cyber-security are absolute certainty, while the benefits of those defences – whether a digital attack occurs successfully – are future uncertainties. The tendency is to not invest and show risk-averse behaviour. In addition, decision-makers may inadvertently be distracted by the symptoms, reducing their focus on hard-to-observe root causes. As a result, investments in other strategic business activities that seem more important prevail at that time. Examples include implementing an important marketing campaign, innovation of the products, services and processes. bringing in a large and unique order, website improvement or opening a new location.

Today's choices unconsciously lead to the problems of tomorrow, possibly with disastrous consequences for reputation, customer confidence and financial costs. Future cyber-security incidents will lead to high costs for correction and recovery for organizations. When a major a data breach manifests itself, the priorities of the organisation change immediately and absolutely. In that undesirable crisis situation, the defending organization is faced with double the cost of investing in necessary, good, cyber-security strategy by having to repair the damage caused by the data breach. Examples of such a situation are countless.

> *Business leaders need clear insight into the short- and long-term consequences of their choices regarding cybersecurity.*

The dynamics of cyber-security

We try to improve our cyber-security with the current, static decision support tools, examples of which are risk management, best practices, standards and benchmarks. These tools only provide a snapshot. They provide insights into the "now". However, the world is fast changing. Today's insights will be outdated tomorrow. A cyber-attacker does not care about a risk assessment; it does not affect him at all. Cyber-criminals do not care whether an organization is compliant. A threat actor does not care about the scope of a security function compared to other comparable organizations. Attackers look for exploiting weaknesses in employees' knowledge, systems, equipment, software, and processes for monetary gain or otherwise.

There is a constant dynamic interaction between the attacker and the defending organization, hereinafter the defender. Both parties look for weaknesses in processes, technology and human behaviour. The attacker wants to exploit this weakness and the defender naturally wants to prevent the same. This dynamic – attacking and defending – is highly turbulent and changing in nature. It may affect business operations and IT and can have significant consequences for the defender's finances and risk management. It may also noticeably affect personnel capacity. However, when one of the parties is successful in attacking or defending, the other anticipates this and adjusts its working method.

Following this dynamic, cyber-security can be divided in four closely-intertwined management challenges that determine the success and performance of the organization:

1. Mastering the defence skills. This concerns the extent to which the defender can identify and resolve weaknesses in employee knowledge, processes, software and digital devices in order to prevent the attacker from exploiting them.
2. Finding the needle in the haystack. This is about the defender's ability to respond to security incidents filtered from observed suspicious signals.
3. Winning the intelligence race. This is the degree to which the defender is able to actively learn from the development of the attacker.
4. Managing growth. This concerns the workload that the defender can handle, taking into account the current business operations, implementation of new, strategic developments and mitigation of incidents.

A successful attack may enormously affect a defender with drastic consequences of correction and recovery. This can often be causally and indicatively traced to the inadequate implementation of these four management challenges.

The dynamics in cybersecurity require proactive, forward-looking risk management to validate the effectiveness of (intended) decisions.

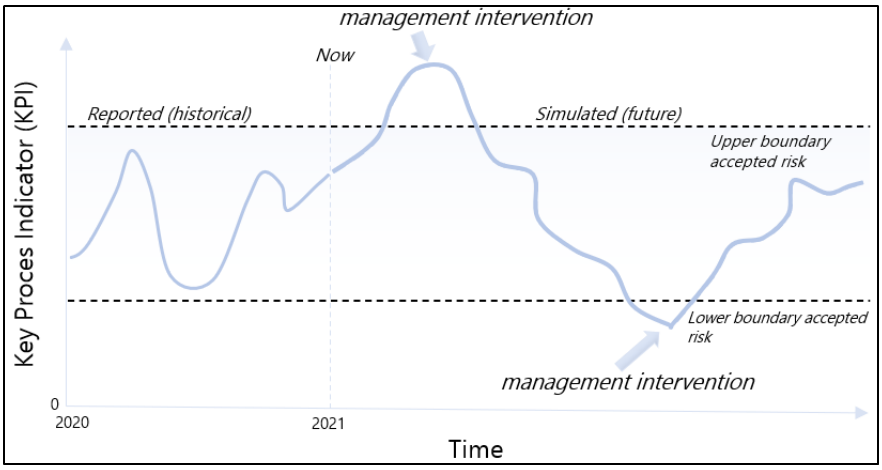


Figure 1. KPI reporting in a context of proactive risk management.

Figure 1 is an example of proactive risk management. This figure shows that future simulated performance indicator behaviour is the basis of decision-making. Decision makers can intervene when accepted risk boundaries are expected to be crossed by this future-simulated performance.

A valid cyber-security strategy

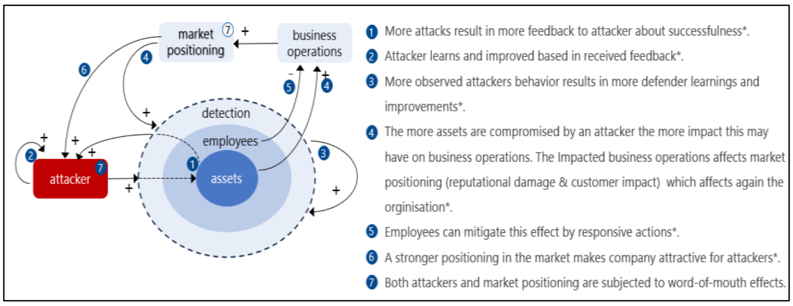
It sounds like a cliché: today's decisions lead to tomorrow's problems and, if you know in advance what is feasible, you don't have to correct so much afterwards. Organizations can no longer afford to "haphazardly" manage their cyber-security posture. Despite this, many organizations inadvertently spend millions, possibly billions, in correction and remediation costs. Decision-making processes in organizations are complex and often time-consuming. After all, many steps and analyses – including but not limited to a plan of action, a feasibility analysis, a business case with financial calculation, a risk management analysis, a resource plan and interdependency analysis – are required before a strategic plan is approved. Organizations often involve multiple specialisms or even departments with their own methods, policies and principles. This may cause consolidation issues of a plan in a later stage.

Implementation is only possible after such strategic plan has been approved. Recruitment and selection of personnel takes time. The same applies for supplier selection. A delivery time of months and sometimes years can be quite normal for such plans. The attacker has nothing to do with this. The attacker has their own higher development speed and more flexible innovation pattern which is less hindered by these delays.

This shows that there is causality within the structure of an ecosystem (read: the whole of people, processes, technology and governance) and the behavior of this ecosystem. The relation between ecosystem structure and its observed behaviour is the basis of the structure-behaviour-paradigm and is an important starting point for dynamic modelling.

Dynamic modelling is a scientific methodology that provides insights in the structure of an underlying ecosystem that causes observed behaviour. Through a combination of algorithm-building techniques, simulating future behaviour performance indicators become visible. Scenario analysis provides insights into how this behaviour can be influenced by policy decisions. This method is perfectly suitable to analyse complex dynamic issues.

The basis for solving these previously-mentioned problems lies in providing insight into the interaction between the attacker and the defender and understanding how those problems subsequently affect customers, reputation and finances. The extent to which an organization can respond to the attacker again depends on the relationship between employees, processes, technology and management. Figure 2 is an example of the insights in such structure.



1 More attacks result in more feedback to attacker about successfulness*.

2 Attacker learns and improved based in received feedback*.

3 More observed attackers behavior results in more defender learnings and improvements*.

4 The more assets are compromised by an attacker the more impact this may have on business operations. The Impacted business operations affects market positioning (reputational damage & customer impact) which affects again the orginisation*.

5 Employees can mitigate this effect by responsive actions*.

6 A stronger positioning in the market makes company attractive for attackers*.

7 Both attackers and market positioning are subjected to word-of-mouth effects.

Figure 2. Example of an ecosystem structure.

The bridge that Disem Institute builds between science and practice is particularly innovative as it ensures that new analysis methods, including dynamic modelling, are available. Disem Institute applies the scientifically validated method of dynamic modelling to the specialist field of cyber-security, allowing it to provide clear and comprehensible insight into the aforementioned interactions and coherence. The Disem Institute approach offers the possibility, by using specific algorithms, to create simulations with forward-looking projections and identify management levers for intervention. The scientifically-validated approach of dynamic modelling by Disem Institute leads to sustainable and effective strategies that support business leaders in their governance practices. It visibly results in fewer repair and correction costs. Business leaders receive clear intuitions regarding what does and does not work with respect to cyber-security strategy at an early stage. These insights can be used for feedback on the decisions and actions that are planned as follow-up. Our approach shows executives the effectiveness of their cyber-security strategy before making large investments and implementation.

The scientifically-validated method of dynamic modelling used by Disem Institute provides insight into how a proposed cybersecurity strategy is developing and shows, at an early stage, which intervention options are available. This insight offers business leaders a solid and well-developed cyber-security strategy.

Literature

Kahneman D., 2011. Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.

Kahneman D., & Tversky A., 1979. Prospect Theory: An Analysis of Decision Under Risk, Econometrica, 1979, Vol 47, No 2.

Moore T., Duynes S., & Chang F.R., 2016. Identifying How Firms Manage Security Investment. Workshop on the Economics of Information Security (WEIS), Berkeley, CA, June 13–14, 2016.

Paape L., 2008. 'In Control' statements: Fried air or a phenomenon to be cherished? Oration, Nyenrode Business Universiteit, 2008.

Paich, M., Peck, C. and Valant, J., (2009). Pharmaceutical product branding strategies: simulating patient flow and portfolio dynamics. Second edition. Informa Healthcare USA. Inc.

Zeijlemaker S., Bening R. & Rouwette E.A.J.A. (2019). Unravelling the dynamic complexity of cyber security investment decision-making. In One Conference 2019. The Hague, the Netherlands

Zeijlemaker S., (2016). Exploring the dynamic complexity of the cyber security economic equilibrium. Colloquium of the 34th International Conference of the System Dynamics Society: Delft, the Netherlands (2016, July 17 – 2016, July 21).

Disem Institute

Disem Institute specializes in analysing complex, dynamic and strategic management issues and excels in the field of digital security. Disem Institute offers the means to see and follow how strategic decisions will occur in an explainable way in the future. Our scientifically-validated approach demonstrates the effectiveness of a strategy before business leaders make large investments.