nixu
cybersecurity.

The ROI of cybersecurity

Does cybersecurity create business value?

WHITEPAPER

WHITEPAPER | October 2019

We recently collaborated with Nyenrode Business University on research focusing on the added value of cybersecurity.[1] How much should an organization spend on security? Are there additional, valid reasons for making cybersecurity investments in your business, other than for risk reduction purposes or managing the costs of an incident?

Contents

Does cybersecurity create business value?

Nixu conducted an extensive analysis on cybersecurity business value, combining expert insights with field research encompassing interviews with Chief Information Officers/Chief Information Security Officers (CIOs/CISOs) of six globally active corporates from the Netherlands which are operational in four different domains: Payments, Retail, Industry, and Government.

The discussions held during these interviews were centered around the following core issues:

- Cybersecurity and risk awareness at the board level
- Stakeholder trust in the company, and the impact that incidents have on this trust
- The creation of business cases for security-related activities
- The validation of business cases, including the ROI (Return on Investment)
- Cybersecurity budget as a percentage of the total IT budget

From incident-driven to value-driven cybersecurity: why, and how?

Through our research on cybersecurity and risk awareness at the board level, we found that CFOs and CISOs rarely focus on business value. Although there is more awareness about cybersecurity risks at the board level today, it remains difficult for boards to quantify cybersecurity risks properly. It has proven difficult for organizations to evaluate cybersecurity risks in the same manner as other business risks, thereby inhibiting their ability to make calculated decisions about security control investments.

The majority of arguments presented by CIOs and CISOs used to justify investments in cybersecurity are:

- adhering to good practices and standards (compliance); and/or
- a CISO's qualitative judgment of the perceived risk;
- examples of security breaches at other organizations and their reported financial impact.

It was concluded that there is a lack of data to evaluate the costs and benefits of security control measures. There are no standard formats for defining the investments, so benchmarking costs and benefits is not possible. It is even difficult to compare data within one industry, let alone amongst several. Identifying the value of security is an extremely complex task.

In our opinion, qualitative input is very rarely a sufficient argument for an executive board to be convinced to invest or increase investments in cybersecurity. No matter how good the qualitative arguments, boards are hardly ever tempted to follow good advice if there is no (financial) business case. However, real examples of security breaches at other organizations are more likely to trigger them.

The Maersk Case

"Could this also happen to us?"

A good example is the Maersk ransomware incident. [2] Many organizations did not consider IT security a realistic business risk. IT security risk was accepted and tolerated (if it was ever classified at the board level). It was only after the Maersk case that the perceived risk was taken more seriously and deemed unacceptable.

We concluded that organizations generally do not prepare business cases specifically for cybersecurity. Cybersecurity's return on investment (ROI) is hardly ever calculated; consequently, companies do not create KPIs based on ROI. Organizations do not sufficiently identify the impact that IT security breaches can have on the public's trust of the organization.

We believe that diverse arguments are required to convince the board of increasing levels of risk. High or very high risks need to be made tangible using quantitative methods or real incidents. The latter is obviously not preferred.

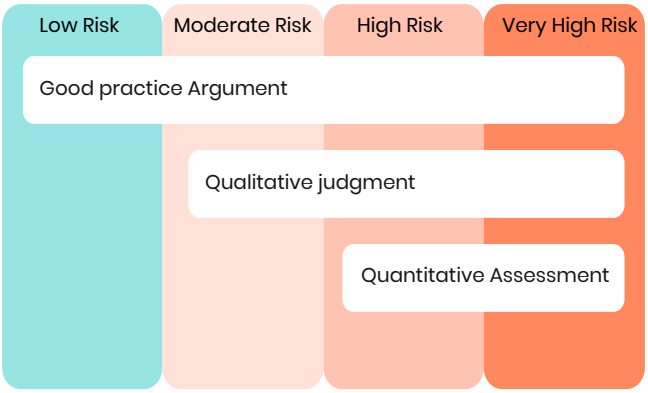

Image 1: Risk perception

Risk Perception

"Management choices are driven by emotion rather than by fundamentally proven reasons"

Getting a grip on ROI

Introducing a maturity model

Based on the results of available research, Nixu developed a Security Maturity model, which defines four maturity levels.

Level 1 Incident-driven cybersecurity is characterized by a technical approach to security. Cybersecurity is an operational 'responsibility' in the IT department of the organization and is based upon best practices or best effort. There is no consistency and no planning. Management will only be involved when a major incident occurs. Security measures are perceived as a cost to the organization. The first level of maturity is, in fact, the firefighting level of security. Every incident is handled as a new experience in itself, nothing is learned from the event.

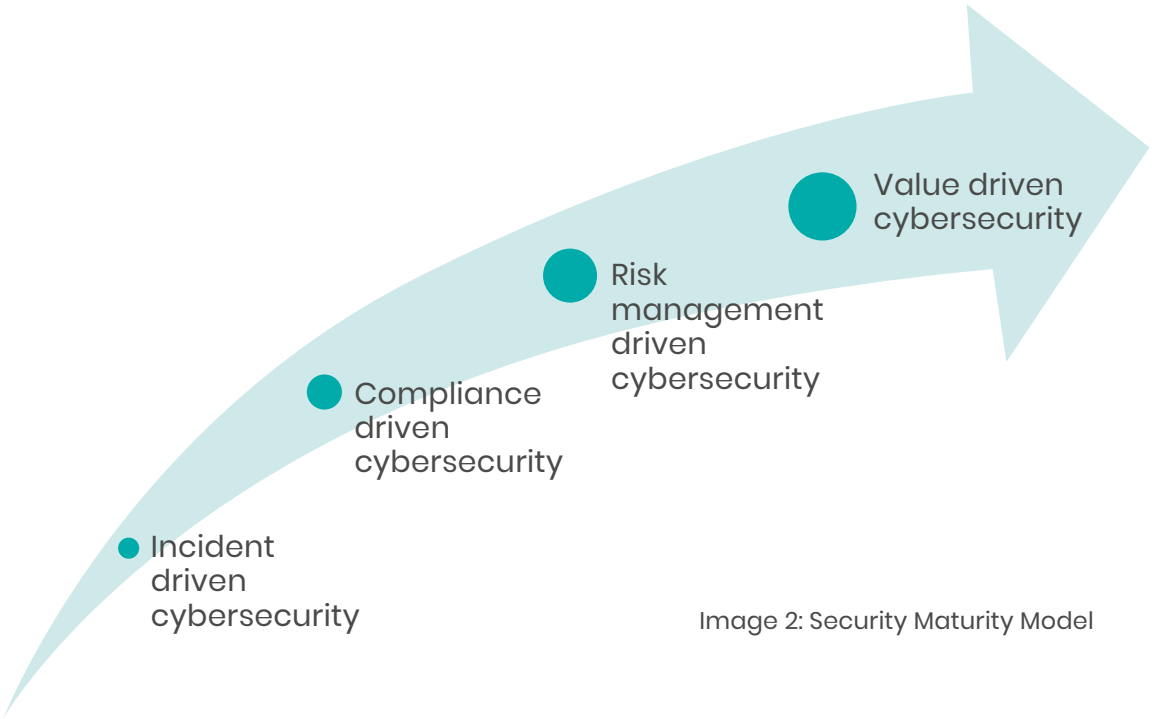

Image 2: Security Maturity Model

Level 2 Compliance-driven cybersecurity is the 'good enough' security level. Which means security control measures are implemented based on security baselines and on the expectancy of compliance or supervisory audits. Costs are of little importance, compliance requires expenditures and the executive board will accept these costs. It's just enough to comply with laws and regulations. Risk assessment, if performed, carries focus on the risk of being non-compliant.

Level 3 Risk management-driven cybersecurity is characterized by organizations understanding their risks and their own need for cybersecurity. Responsibility ownership is typically deployed higher in the organization. Cybersecurity is aimed at managing security to mitigate risks. Since risk management is an eternal process, and risk management is about prioritizing and planning, multi-year planning and budgeting processes are essential. The budget will be allocated based on priorities, but security is (still) seen as a cost for the business.

Level 4 Value-driven cybersecurity is characterized by organizations using their level of cybersecurity to generate revenue. Cybersecurity actually becomes a business catalyst, as it can be a unique selling point in markets where cybersecurity is not typically included as a service feature. Clients and business partners engage in different levels of cybersecurity, which supports additional revenue generation. Organizations on this level should be able to calculate their own ROI.

The security maturity model can be used to assess the current maturity level of an organization and it can be used to set a strategic target state. In our model, the security maturity level is determined based on the following type of questions:

- Is there a business case for security investments? (level 4)
- Does an annual security budget exist? (level 3)
- What are the costs incurred by security activities? (level 2)
- Are you surprised by the costs of security incidents? (level 1)

Security – an intangible value

A well-developed security infrastructure must be viewed as a valuable asset. It could be compared to the economic value of goodwill, which is a by-product of sound entrepreneurship. Goodwill is the intangible value of an organization consisting of the future economic value of reputation, customer relations as well as product and services quality. Security can be addressed in the same manner: the intangible value of the security investments of an organization, lower operational risks, and the opportunities for future growth based on reputation and process, service and product quality.

Ambition definition

Based on the field research conducted, it was concluded that organizations have varying levels of ambition for security maturity. The majority of organizations may not aspire to achieve Level 4 maturity. As long as security is seen as a necessity, level 3 may be the best level. Reaching the highest level of maturity (4) monetizes IT security, requiring a mature security infrastructure and hefty investments. For instance, a security certification is required, which is an expensive procedure that only needs to be performed if a company strives for market presence. In our opinion, a security certification (such as ISO27001 or SOC2) is the gatekeeper of level 4 maturity.

Move up to level 3 and 4: A strategy and roadmap

Based on the research, we draw the conclusion that most organizations are on the maturity level 1 or 2, but have the desire to mature towards level 3. In order to reach the 4th level of maturity, a long-term strategy in the form of a roadmap is needed. How can you get there? We offer a step-by-step approach towards the desired maturity (image 3).

Cybersecurity strategy

The Strategic Alignment Model (SAM) proposed by Henderson and Venkatraman [3] is one of the most cited strategic alignment models for aligning IT and business strategies; additionally, it is useful for aligning the cybersecurity strategy. A business strategy is defined as business scope, distinctive competencies, and business governance. We define a cybersecurity strategy as technological scope, systematic competencies, and information security technology governance. In a mature organization, the business strategy drives the IT security strategy, and this in turn drives the IT security operations.

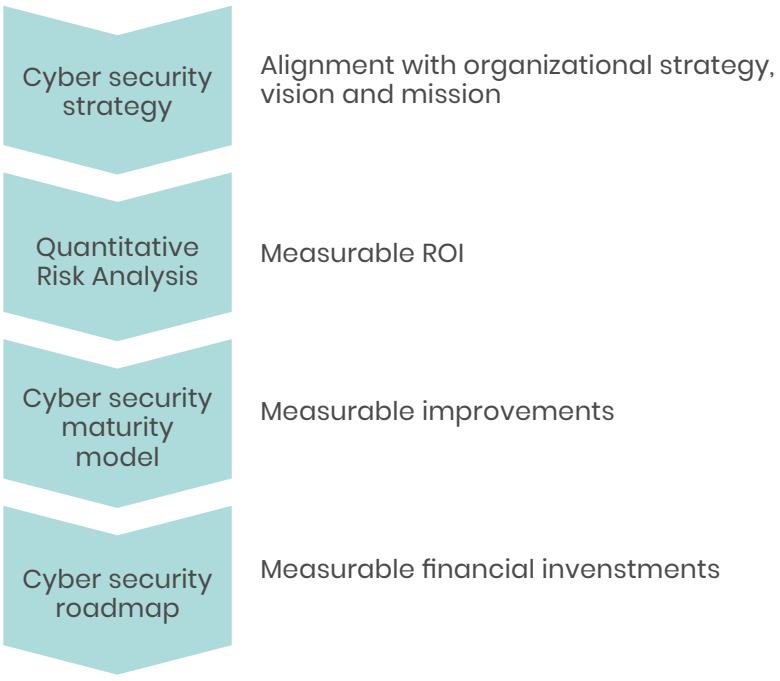

Image 3: Nixu Cybersecurity Roadmap

Quantitative risk analysis

The ability to perform quantitative risk analysis is necessary to mature to level 3 or higher. Specifically, the high risks need to be quantified, to support cost-benefit analysis.

Cybersecurity Budgets

"If you could help me calculate this budget,
I will owe you for life! I could try myself,
but I just know it won't be very accurate"

We have developed a quantitative risk approach [4], to help enable organizations make their most important cybersecurity risks, their investments and their ROIs measurable. Quantitative risk analysis is a proven method used by banks and insurance companies to estimate financial risk, but it can (and should) be equally applied to cybersecurity risk. This method will provide insights into the expected annual loss due to risks. Likewise, the effect of mitigating control measures can be calculated. An example is given in Figure 4, where the blue line represents the inherent risk and the green line represents the risk after applying new security control measures. The risk analysis essentially reduces information-related risks to an acceptable ratio of risk to cost. Implementing the quantitative method can help calculate expected losses and the ROI of security investments.

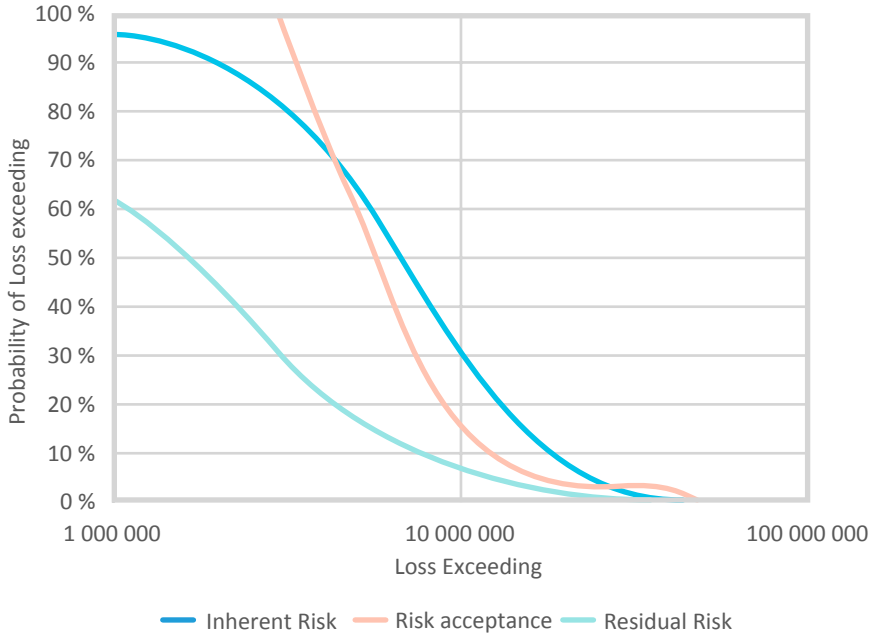

Image 4: Expected Loss model

Cybersecurity Roadmap

Based on the strategy, risk analysis and the required maturity, a cybersecurity roadmap can be designed. The roadmap should contain goals, new capabilities and planning. Goals are both short and long-term achievements that the organization outlines with a solution roadmap. Specifically, the goals will focus on reducing risk and augmenting the cybersecurity maturity. New capabilities will be provided via enhanced systems or processes. Planning includes timelines, resources, and detailed budgets.

Final thoughts

Some organizations may not see the necessity of calculating the value of Security as an Asset, but if they do, a roadmap to maturity can be created using the maturity model. If organizations want to use their cybersecurity abilities to compete in the market, the ROI of any security investment should be calculated. Then, just like goodwill, the value of security can be seen as an asset, making it a topic for board members to make calculated decisions.

We expect to be able to offer more insight into the costs and benefits of security once more data is available. However, every step will have a significant impact on the Cybersecurity Operating Model. The risk perception view (see image 1) can help generate awareness that is essential for board level support. By following our roadmap, including quantitative risk analysis, organizations are enabled to move from incident-based or compliance-based cybersecurity to risk-based and business value-driven cybersecurity. Having reached this level, they can perform cost-benefit evaluations and use Security as an Asset.

About us

Please contact us if we can assist you in making your cybersecurity risks measurable and more comparable with your other business risks. Our combined quantitative and qualitative approach helps executive boards across Europe with their risk assessments on a daily basis, and was specifically designed to bring business value to your cybersecurity program.

Nixu is a listed company with a 100% focus on cybersecurity. We were founded in Finland, where we have been active since 1988. In the years since, we have expanded throughout the Nordics and into the Benelux region. We provide the full lifecycle of security solutions, from consultancy to implementation, monitoring and support. What makes us unique is our focus on the combination of strong business and vast technical skills.

References

[1] Keshari, S. & Kurulkar, C. (2019). Thesis: CYBERSECURITY VALUE PROPOSITION FOR NIXU B.V. Nyenrode University.

[2] Greenberg, A. (2017). How Shipping Giant Maersk Dealt With a Malware Meltdown. Wired.
Retrieved from https://www.wired.com/story/petya-ransomware-news-roundup/

[3] Henderson, Oldach & Venkatraman (1993). Strategic Alignment Model.
Retrieved from https://www.valuebasedmanagement.net/methods_venkatraman_strategic_alignment.html

[4] Van den Hooven, C. (2019). Quantitative approach of Risk management. CISO says. (1-4).
Retrieved from www.nixu.com/insights

NIXU cybersecurity.

Contact

/nixuoy
@nixutigerteam
/company/nixu-oy

nixu.sales@nixu.com
www.nixu.com

Nixu is a cybersecurity services company on a mission to keep the digital society running. Our passion is to help organizations embrace digitalization securely. Partnering with our clients we provide practical solutions for ensuring business continuity, an easy access to digital services and data protection. We aim to provide the best workplace to our team of nearly 400 cybersecurity professionals with a hands-on attitude. With Nordic roots we serve enterprise clients worldwide. Nixu shares are listed on the Nasdaq Helsinki stock exchange.