# Discussing information security with the board of directors

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Given the growing importance of data and IT systems for businesses and the growing number of vulnerabilities, cyber threats, data beaches and cyber security regulatory landscape, information security has become in recent years a topic that should be addressed at the level of board of directors. This is relevant for both SMEs and large corporations.

According to a recent study, respondents asked what puts the highest pressure on cybersecurity management responded competition for budget (46%) and security of attacks (49%). Thus, the management of security risks, including prioritization, budget and management buy-in weight almost as much as the ever changing security threat landscape.[1]

## 1. What content to present to the board of directors?

Usually, investments numbers for all initiatives are considered in relation with revenue numbers or cost savings/avoidance that support the company strategy. If we regard the IT risk related initiatives as just hygiene, they will not be taken as a compelling call for action, but at best as an urgent fix (such as wearing a mask or washing the hands, these days) and at worst as not necessary or not now.

The usual reasons for IT security investments are related to potential negative impacts from fines, and this was even more so after GDPR legislation enforcement. Reputation hits after data leaks or successful hack are easier to imagine, since there were (in)famous incidents that are globally known, due to their big impacts. The loss of productivity is also considered with the systems unavailability. With exercises such as ORSA, these types of impact can be quantized in money so the conversation becomes more intuitive and the relation with the organization's objectives more clear. All these need strategic decisions and investments only the board of directors can take and decide accordingly.

Prevention is likely less costly than remediation, thus the board of directors has to analyse opportunity of a cost avoidance decision through the implementation of certain security controls or items in the security programme.

[1] 451 Research, commissioned by Kaspersky, "Cybersecurity Through the CISO's Eyes: Perspectives on a Role"

Generally, loss of clients' trust is more damaging to revenues than the budget needed for the security investment required.

In B2B commercial relationship, security is actually considered both as risk evaluation and as professional assessment of existing measures. In a competitive bid, there are RFP check lists that an organization passes or not, thus qualifying for new business proposals.

So, how do we show all that in a convincing presentation to your executive board?

That depends on the organization's objectives, on defined (or not defined) risk appetite and the board members experience with security concepts understanding.

Considering these, you need to choose the "money only" argument and / or the risk tolerance reason and / or the market security best practices. [2]The arguments are there, the cause is worthy but the best suited plead is the one that fits your audience best.

Thus, the main pain-points encountered relate to differences in terms and presentation angles used by the board and by the information security team (e.g. CISO). In this respect, the following main environmental aspects have to be taken into account:

**Specifics of the organization's business field:**

The approach to be taken in discussions with the board depends on the industry in which the organization acts, as organizations in certain industries may hold extensive amounts of data and/or complex IT systems or infrastructures, whereas other industries may hold less data and/or have less complex IT systems or infrastructures.

**Maturity level of the organization:**

Further, this approach depends also on the maturity level of the organization in terms of security and information technology. For each level of maturity, the CISO has to take into account the existing internal processes, the maturity level of other areas within the organization, the organization culture in terms of technology and security and adapt proposed improvements accordingly.[3] Not having the maturity level in mind may lead to inadequate proposals, as the building blocks necessary to implement the new proposal do not exist yet in the organization. For instance, if the CISO wishes to implement a SIEM solution, but some of the IT systems within the organization do not record proper logs, the CISO should first focus on proper logging of relevant aspects for each IT system.

[2] https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask/ , last accessed on 15 April 2021.
[3] ENISA, "NIS Implementation Report", 2020.

**Team contribution:**

As information security does not exist in isolation from the other areas within the organization, security proposals should have in mind the impact in such other areas. Aside from the business objective, which is essential, some of the most relevant areas with which the CISO has to coordinate for information security projects are the operational side of information technology and the data protection officer. This ensures correlation with other initiatives within the organization and support from the teams that will be involved in the implementation of the project.

## 2. How to discuss with the board of directors? Approach tips and tricks

**Continuous updating on projects:**

Create a list of current and finished projects since the last meeting and explain how they have positively impacted the company. This ensures that management understands the relevance of information security for the business objectives and, also, the progress that have been and that remains to be made in this respect. Of course, non-technical, summary presentations should be used. Thus, the emphasis should not be on the budget amount for the security projects, but, rather, the status within the security plan based on the agreed security strategy. It is useful for management to understand from a quantification perspective, how the organisation is more secure than previously. The quantification may include types of vulnerabilities closed together with their business impact, number of incident alerts generated for specific vulnerability exploitations.

**Non-technical language:**

The topics to be presented before the board of directors should not be at a granular technical level, but, rather, at a high-level, outlining the business impact (and regulatory, if the case). Thus, the presentation should be aligned with the business goals and reflect business perspectives so it will reach the business people we have as audience during our presentation, with emphasis on information security risks with high impact and probability from a technical perspective and from a business perspective.

The consequences related to risks should be presented in a measurable manner. For certain consequences, the calculations may prove to be difficult.

For example, for a penetration testing report, the presentation should not outline the technical vulnerabilities identified and the technical consequence mentioned in the report together with the probability mentioned in the report. In terms of probability, the report is originally created in the context of the penetration testing and may need to be adjusted having in mind the methodology used by the organization to calculate probability and having in mind the entire IT infrastructure

and security controls in place. Furthermore, a general consequence of data leakage is not sufficiently clear for non-technical individuals, such as the members of the board of directors. In this case, additional context on the criticality of the systems affected and the consequences based on the data affected should be detailed as quantifiable as possible.

**Focusing on risk overview**:

This can be achieved with emphasis on specific, measurable impacts on the business or on the organization. As per a survey conducted by ISACA, only 21% of senior management is briefed on risk topics at every senior management meeting.[4] Thus, the technical analysis and specific technical pain points are useful. However, in terms of presentations before the board of directors, emphasis has to be placed on impact and probability of a risk, with such risk being described in plain language and not technical jargon. The risk-based approach highlights that information security is not a one-off exercise and not just a question of compliance with legal/best practice requirements, but an exercise of risk assessment and risk mitigation in a continuously changing environment.

**Preventive vs. incident costs:**

This depends significantly on the type of incident. For certain types of incident estimations may be made – e.g. recovery from ransomware where no data exfiltration occurred. But for most incidents, aside from the vulnerability fixing and disaster recovery steps (which relate to actions taken by the company itself), other costs/damages/fines that may be incurred by the organisation can prove difficult to calculate. Nevertheless, this comparison can be used in certain specific situations. In terms of comparison of costs for implementing controls, one might try to make a comparison between the costs for control implementation and the costs for investigating and remediating an incident.

The information on incident costs may be obtained from previous incidents, bug fixing activities, vulnerability fixing activities and market statistics on incident fixing costs. On the financial side, indirect damages, such as loss of productivity due to downtime, loss of sales can also be taken into account for the relevant calculations.

It is difficult to establish value of data in an IT system, but criticality for business may point in the right direction. Insurance companies themselves have just started in the last decade to explore more comprehensive models for calculating cyberisk in view of calibrating their insurance products.

[4] ENISA, "Survey Strong tech governance drives improved business outcome", 2017, https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2017/survey-strong-tech-governance-drives-improved-business-outcomes , last accessed on 4 April 2021.

**Benchmarking against other companies**

This type of analysis (especially in the same sector) is often requested by management. However, this is difficult and tricky in practice. In terms of governance and risk management, such information is not publicly available. Even if, for instance, the budget amount for information security would be mentioned in the financial statements of the competitors, this does not detail the internal steps taken, nor the risks assessments performed by the organization. In terms of incident handling, public information is scarce, without proper information on costs or mitigation actions taken. The only relevant information that may provide guidance on certain trends is included in various data breach costs or security posture surveys performed in the market. Nevertheless, these can provide only limited informations about the trends in terms of information security, with the internal strategy and approach to be decided by the organization based on its specifics.

For controls related to incident identification steps and early response in case of incidents, quantification of the breach costs reduction may be useful to be included in the business case.

**Statistics about past events:**

Management generally asks about number of data breach for a particular IT system or type of vulnerability as a manner of calculating the probability of a risk occurring. This may be included as insight into presentation of risks, however, it should not be relied on as a metric in this respect. In the same manner, management inquires about financial loss, fines or damages incurred in the past by the organization (or other entities in the market) for a specific type of vulnerability exploitation or security incident. This may be factored into the decision about risk response, however, it is not necessarily relevant, as these are not indications about future situations, which may differ based on consequences of the incident, evolving threat landscape and evolving guidance and requirements in terms of level of security to be implemented by organizations.

**Hands-on testing:**

Testing incident response and business continuity/disaster recovery processes together with relevant stakeholders and the board of directors can also help with further understanding of information security risks and potential consequences of the occurrence of such risks. Given that the testing involves use cases from real-life scenarios together with role-playing and detailing of business impact, it is a good approach towards more information security awareness among the board members.

**Certifications**

These are useful in terms of client's perspective on the organization and in order to ensure standardization and state of the art process in place within the organization. One approach that may be easy for management to relate to are the steps to be implemented in order to achieve a security certification, which generally helps also with increasing the maturity level of the organization. Therefore, information security may also be used as a selling point for the organisation in terms of branding, showing the effort the organisation makes to ensure security

and privacy of its customer data. Certification has to be viewed in correlation with the maturity level of the organisation in terms of information security.

Further, in case of service companies or highly regulated sectors, certification (especially ISO ones) are starting to become the norm, with large demand from relevant stakeholders and authorities in this respect.

**Risk appetite calculation:**

The risk appetite established by management should be based on proper knowledge of the threat landscape and the security posture of the organisation by reference to risks identified and evaluated. This ensures that proper risk appetite is chosen by management and this is the key in setting the tone in information security within the organisation. The role of the board is to set the direction of the company and make the decisions in terms of business development and operation, while taking into account all compliance, legal, security risks and without going into details about the day-to-day operational activity.

**Cooperation in cybersecurity:**

Management has to be aware of the need for cooperation in ensuring information security. Information security is not achieved with effort solely from the IT security department, but also from other departments from IT operations, IT development, legal, compliance, risk management, data protection, business owner, audit etc.[5] For this reason, for each initiative presented before the board of directors, proper emphasis has to be placed on the internal skills and departments that need to be involved in the initiative. This includes also reliance on and dependencies with vendors, in terms of request for proposals needed, additional services that should be added to existing agreements, special SLAs for information security and business continuity, proper liability and undertakings clauses etc. Emphasis should be placed on the resilience that is provided to the organisation through the information security steps taken.[6]

Provide insight into the need for orchestration of people, processes and technology in order to ensure information security, while underlining the role of the board of directors in this respect.[7]

[5] Khalid Kark, Caroline Brown, Jason Lewris, Bridging the boardroom's technology gap, Deloitte University Press, June 29, 2017

[6] World Economic Forum, Principles for Board Governance of Cyber Risk, Insight Report, March 2021.

[7] RSA, "Security and Risk: How to talk digital risk with the board", https://www.rsa.com/content/dam/en/analyst-report/gartner-how-to-talk-digital-risk-to-the-board.pdf , last accessed on 15 April 2021.

**Preparing the meeting with the board of directors**

Before making the presentation before the board, it is useful for all the matters to be discussed with the relevant stakeholders beforehand in detail, so that each stakeholder is aware of the risks and the proper internal security assessment process has been completed. Having all relevant stakeholders involved in the risk assessment and risk addressing already knowledgeable can bring clarity to the discussions with the board of directors and relevant (and measurable) input for the CISO to prepare his/her presentation before the board of directors.[8] This also ensures that each stakeholder understands its role in the information security program, especially those that are responsible for taking appropriate steps as per the relevant RACI matrix.

The responsibility of each stakeholder (e.g. business owner) about information security control implementation ensures that security is included in the project budget, such as budget for initial and periodical penetration testing and for periodical vulnerability assessment. This leads to swift implementation of appropriate controls and consistency in budgeting methodology between business changes and information security controls. The alternative would involve approving a specific budget for the security department and may lead to situations where the budget does not match the actual needs of the business. Further, it useful to have in place a cyber-risk management process that interacts with the operational processes.

Further, a correlation with the business objectives and alignment with these should be implemented.[9] In addition, an approach in this direction is to link top initiatives to top business risks.

There is regulatory landscape on security (in certain domains such as banking, insurance, energy, entities falling under the NIS Directive), there are also implications of GDPR in terms of security steps to be taken. Nevertheless, in most cases, the legislation provides the aim of the security steps to be taken by organisation, but leaves the specific operational approaches to be decided by each organisation, based on their structure, activity and IT landscape.

A balanced score card can be used to outline the financial aspects of security (e.g. supplier management, efficiency in internal security management with task allocation mechanisms, use of security to grow the business and reach business objectives), customer (availability of service, security of data, confidence and trust in the services offered by the organisation), operational (proper IT solutions and automation, proper change management process) and human factor (proper awareness of risks).

[8] Tony Kontzer, "C-suite cybersecurity awareness may be the key to taking a bite out of breaches," RSA Conference, July 19, 2018.
[9] Isaca, "Reporting Cybersecurity Risk to the Board of Directors", 2020.

Thus, when analysing the risk impact/probability and the risk acceptance, compliance with legal provisions, potential fines/damages, business impact and trust of clients should be considered. In this respect, the business strategy can use the security controls in place.

The risk addressing proposals and any improvement in the information security program should outline three different approaches:

a. Minimum: This option presents the bear minimum requirements that can be implemented efficiently within the given budget. It often includes only critical risks or legal requirements with more impact in terms of risk mitigation.
b. Moderate: This is often the option chosen for implementation. It goes beyond the bear minimum requirements and more towards state of the art ones. However, it is based on the level of maturity of the organisation and a balance between the potential benefits it can bring and the investment it requires.
c. Bullet proof: a solutions that includes state of the art implementation of all requirements and best practices. Often this solution entails huge costs, which have to be analysed by reference to the benefits it brings to the organisation (either profit or reduction of potential losses/costs).

What-if scenario based on each of the three approaches is highly desirable to reveal the organisation's risk posture including possible financial losses.

The request for board decision(s) should be clearly articulated and should emphasize security team's recommendation(s). This request should touch briefly the following structure – organisational change required, program/project/project change required, training/awareness required, investment required, and nevertheless what are the costs required for implementation.

Nevertheless, the controls to be set in place (technical, organizational or other types) should be presented in a measurable manner, outlining the risk reduction level, any cost or FTE reduction and any dependencies on other departments or assistance needed from other departments in the organization.

**Frequently asked questions by the board of directors**

The below presents certain types of questions that are often asked by the board of directors when faced with information security decisions.[10] We have include a short recommendation for approaching these. Nevertheless, the specific factors concerning the organisation's business sector,

[10] RSA, "Security and Risk: How to talk digital risk with the board", https://www.rsa.com/content/dam/en/analyst-report/gartner-how-to-talk-digital-risk-to-the-board.pdf , last accessed on 15 April 2021.

security maturity level and structuring have to be taken into account in order to best address such questions and provide relevant information to the board of directors for an informed decision.

- Can this be automated?

Explain what can be automated and what cannot. Further, detail what are the advantages of automating certain steps in security or in other business process to reduce cyber-risks, but also highlight the areas where automation cannot bring added value by reference to its costs and the areas in which automation can increase exponentially operation risk if not implemented properly.

- How should we approach this risk?

Explain the business impact of each risk and the risk response options from the response that best suites business needs to the ones that best suit security/risk mitigation needs.

- What are our options?

Generally, the board of directors would like to understand the limits to what can be implemented, both in terms of the minimum controls to be implemented for partial mitigation of the risk, a moderate option that includes best cost-benefit balance and bullet proof option that eliminate all or most of the risk, but may be very costly and time consuming to implement.

- We thought this was already taken care of. Why is this a recurring point in our meetings?

Explaining that there is a constant change in the IT and security landscape, with new threat, vulnerabilities and changing organisation IT systems. Further, for certain risks, the risk mitigation process may take multiple steps to complete all controls that can be implemented.

- Are we 100% secure against all type of threats?

The threat landscape changes daily. The best approach in this scenario is to prioritise the items with the highest risk rating first and take into account the organisation's risk appetite.

- Are we secure against incidents similar to the ones incurred by our competitor?

One cannot speculate about the root cause of such incidents. Most of the information about the incident, causes and consequences is not made public. Only official information stated by the company or authorities can be mentioned and taken into account.

- Do we know our risks? How can we have better insight into our risks?

This is the moment to emphasize any shortcomings in the risk assessment process and to request improvements. Detail the role of each stakeholder involved in the risk assessment process and concrete steps going forward.
Further, highlight that the risk assessment process has to be done periodically, given the changing threat landscape and the changing landscape within the organisation itself (e.g. new IT systems, new products, new processes).

- How did this happen?

Explain the facts, the root cause and how these could not be prevented based on the controls in place and the risk assessment/risk addressing mechanisms in place.

- Why are we spending so much?

Provide constant feedback in terms of progress in information security projects/programmes and their impact on/correlation with business objectives. This helps the board of directors to understand the need for continuous investment in information security, given the continuous changing variables taken into account for the information security risk assessment process.

**Conclusion**

The main take away is to have continuous focused discussions with the board of directors and to ensure emphasis on the risk-based approach for prioritisation of steps to be implemented from an information security perspective.

The discussions can be supported by key indicators on the implementation process, in terms of correlation with best practices and with potential costs, damages and losses.

The continuous feedback loop ensures on the one hand that the board of directors is aware about information security risks when taking decisions and, on the other hand, provides further alignment between business objectives and information security goals/steps, while including all relevant stakeholders in the decision making process.