IT Security: Factors of a Successful ISEC Strategy

INSIGHTS by LEXTA // Denny Roesicke, Marcus Schwertz

In recent months, there have been successful cyber-crime attacks on companies across Europe - despite or perhaps because of the COVID 19 pandemic. Increasingly, medium-sized companies are also being targeted.

Often, information about these attacks must be published by the affected companies, which, in addition to the original damage (production standstill, no sales, no deliveries, etc.), can lead to massive reputational damage and uncertainty among customers.

Therefore, it should be a current imperative for all organisations to critically review the security strategy again and to explicitly communicate the importance of a functioning information security to the management.

The implications and parameters for a comprehensive information security strategy (ISEC strategy) are:

- The increasingly faster innovation cycles and the ever-growing IT penetration mean that malware, and specifically ransomware and other threats, can spread ever more rapidly and along previously unknown paths, which increases the negative impact. The question is no longer if, but when a security incident will occur - a direct attack on information security.

- Organised crime, state intelligence agencies and competitors are "displacing" the classic hackers and web activists. Targets are specifically selected according to the perpetrators' "needs", for example in terms of potential ransoms or technologies to be captured. One can even speak of a special "industry" in which many small "companies" (with mostly 5-15 "employees") are active.

- The attacks are becoming increasingly sophisticated and elaborate: Advanced Persistent Threats, Spear Phishing, Business Process Compromise attacks and Social Engineering attacks - the amount of company-specific threats and attacks almost doubled in Germany in the last twelve months. This is not a German issue alone however with global attacks running into the 10’s of millions each year.

- Only a coordinated approach with many parties involved, both state and private entities, can at least partially reduce the risks resulting from this threat situation. Legislators have also recognised this and are regulating ISEC aspects more and more extensively, for example within the framework of the CRITIS legislation.

Against this background, the "neglect" of information security by management often observed in the past is just as fatal as a pure focus exclusively on the aspects of IT security as a subset of information security. For ISEC practitioners, general principles such as "as much security as necessary, but as little as possible" have long since ceased to be sufficient to align their actions with management's intent. This includes a company-wide shift in thinking from prevention to resilience - considering all aspects of the business. Just as threats are becoming more targeted, the ISEC strategy must be specifically aligned with the needs of the company.

(Resilience: In general, cyber resilience focuses primarily on security aspects and the situation immediately after a cyber-attack).

An information security strategy essentially pursues the following purposes:

- Specification of "guard rails" regarding the establishment, adaptation and control of information security in the company.

- Mapping of the company's risk strategy in terms of appetite and risk aversion

- Definition and delimitation as scoping and prioritisation of information security ("self-image")

- Representation of the awareness of the company management for information security in the sense of a "commitment" to introduce and enforce the contents of the ISEC strategy

As a result, the ISEC strategy is the standard of orientation for those responsible for information security. This enables them to better fulfill the mandate given to them by the management, as the management's intention is clearly expressed.

The information security strategy consists of four elements, which build on each other.

- Based on an assessment and analysis of the situation (1)

- the requirements for information security (2) are identified,

- then the concrete, company-specific principles and goals for information security (3) should be established.

- To be able to implement these goals, the organisational and resource-related framework conditions as well as guidelines for implementation and control (4) should be mapped.

The respective components are detailed below.

1. Analysis of the business environment

The first element is an analysis of the implications of internal business requirements, the requirements of relationships with other parties (suppliers, customers), industry specifics and the requirements and expectations of the business environment, such as shareholders and legislators. The core question of this area is: "What relevant framework factors exist for information security management in the company?" For this purpose, audit questions can support a quick and sufficient assessment:

- **Internal business requirements:** The relevant implications for the ISEC strategy should be identified from the corporate strategy and the associated sub-strategies and other statements by management (e.g., annual report). Is the company planning to open up new markets (travel activities of particularly vulnerable personnel) or to set up a production line abroad (increased risk of industrial espionage)? Are new technologies (IoT devices) to be used in the future? What special features (location of plants) result from the corporate structure?

- **Requirements from relationships with other companies:** What (contractual) challenges arise from the connection with other companies? Are there specific obligations from agreements and contracts? Do IT service providers also need to be managed from an ISEC perspective?

- **Industry specifics:** Are there any special requirements with regard to the company industry, for example through requirements of the industry associations?

- **Requirements and expectations of the business environment:** Is the company subject to certain regulatory requirements, such as the GDPR, the protection of secrets, and others? What are the implications of current adjustments to existing legislation? Are there any challenges from among the shareholders?

2. Information security requirements

Based on the description of the situation, the resulting implications are set against the fundamental threat situation of the company. For this purpose, a consideration of the general and the company-specific threats at the strategic level is necessary. These requirements basically express the respective focal points from the management's point of view regarding the respective risks. These result, among other things, from the degree of digitalisation of the business processes, the diversity of information in the company (production and development data, personal data) and the scope of technical and organisational interfaces to external bodies.

The comparison between the implications and the threat situation leads to requirements for information security in three dimensions:

- **Internal requirements:** What are the priorities for information security? Do certain assets, information or business processes represent the "crown jewels" of the company, which must be protected as a matter of priority, such as development data? Does the company want to position itself publicly in the market as a "secure" company? These are all essential questions in the development of an ISEC strategy.

- **Requirements for suppliers, service providers and customers:** How is information security included in the relationships with direct and indirect participants in the company's value chain? Do corresponding agreements need to be adapted in the long term? Which ones need to be prioritised?

- **Requirements for third parties:** Which ISEC-specific requirements should be considered when working with third parties (regulatory bodies, the public), such as a regular exchange within the framework of an industry working group?

3. Principles and objectives for information security

The information security principles and objectives translate the requirements into long-term, specific, (partially) measurable, achievable, realistic and time-bound objectives (SMART). These objectives provide the framework for the future direction of information security and should provide an approach for those responsible to answer the following questions:

- What should be protected?
- How should it be protected?
- How should the system be improved?

To this end, goals should be mapped in the following areas in particular (these are possible suggestions that should always be adapted to individual needs):

- **Dealing with risks:** "Information security management ensures that risks are regularly recorded and assessed for each relevant asset. In doing so, a cautious view of the effects and a high-risk aversion of the company are to be assumed as a matter of principle. Risks are to be mitigated or insured against as far as possible."

- **Protection requirements:** "The protection requirements of the assets must always be aligned with the respective effects on the higher-level business process. The central value creation stages have the highest protection needs, especially the manufacturing and development processes."

- **Prioritisation:** "When establishing an information security management system (ISMS), the core business processes should be considered first, followed by the support processes. In doing so, development has the highest priority."

- **Clear definition of information security:** "The company's information security management takes into account all information in the group with the exception of the strategic business area 'C', which sets up its own ISMS due to its specific requirements. The respective CISOs are responsible for the interfaces."

- **Requirements from the ISEC perspective for other (sub-) strategies, e.g.:** "Those responsible for the strategic development of the divisions ensure that information security aspects are adequately taken into account in the division strategies."

- **Reporting:** "The ISMS shall provide for quarterly reporting to management based on a key performance indicator system, taking into account implications from other areas, such as production damage incurred."

- **Awareness and consciousness:** "Our employees are regularly trained and educated with regard to current requirements and contents in a target group-oriented manner. Furthermore, there should be an appropriate awareness of information security by practicing open communication and transparency within the company. Reporting information security incidents must not lead to negative consequences for the reporter simply because he or she has drawn attention to the incident."

- **Principles of cost-effectiveness:** "Those measures shall always be selected that provide comparable protection at lower cost than the alternatives."

By setting a corresponding target, the value of information security is established from a strategic point of view. At the same time, it also answers the key question of when a company considers its systems, processes and (information) entities to be "secure".

4. Framework conditions

Within the framework of this chapter, the general conditions for information security management are to be defined in terms of positioning within the company organisation, reporting paths, cooperation with other areas and resources:

- Position of the information security officer (CISO).
- Definition of the authority to issue directives and demarcation between implementation and control, e.g. that the implementation of the principles is the responsibility of the divisions and that the ISEC officers provide assistance in this regard.
- Relative resource allocation (e.g. as FTE per 1,000 employees).
- Reporting paths for regular reporting on information security, the ISMS and the corresponding ISEC communication (regular employee information).
- Integration of information security into the principles of action and management (governance).
- Cooperation with other areas (compliance / internal audit, works council, data protection officer, IT department).
- Control of information security management by the management.

Wrap-up

In order for an individual ISEC strategy to be successfully implemented, several aspects should be taken into account during its creation. In particular, congruence with the business strategy and a long-term orientation are critical success factors for a "good" information security strategy.

At the same time, care should be taken to ensure that the required level of security also "fits" the company - many of the requirements set in the financial sector are simply not feasible in large parts of the SME sector. This also goes hand in hand with acceptance by the employees. Accordingly, the ISEC strategy should also be formulated and supported by the management. This also includes the enforcement of compliance and a corresponding "chain of custody" as well as the allocation of responsibilities to suitable role holders.

The following criteria should be seen as further success factors for the information security strategy:

- Focus on strategic aspects
- Clear mapping of priorities
- Feasibility of requirements and goals

Such a company-specific information security strategy provides orientation and assistance for those responsible for ISEC and represents the elementary umbrella for an efficient and effective encounter with the future more complex challenges and threats to information security - and thus to the company as a whole.

Denny Roesicke

Denny Roesicke joined the LEXTA team after completing a master's degree in business informatics and since then deepened his knowledge in the fields of IT security, data protection and strategic IT management. He is a certified Information Security Officer (CISO) and Deputy Head of the LEXTA IT Security product development group.

Marcus Schwertz

Marcus Schwertz studied Business Administration with specialisation in Information Systems at the European Business School Oestrich-Winkel and the Aarhus Business School as well as Business Administration at the University of Mannheim. Marcus is a certified ISO 27001 Lead Auditor / Auditor, Data Protection Officer DSB-TÜV and Data Protection Auditor DSA-TÜV.

LEXTA

is a consultancy company with focus on strategic IT management and offices in Germany, the UK, Austria and Switzerland. Founded in 2003 as an IT benchmarking specialist, LEXTA's competencies since then have broadened and include sourcing advisory, security advisory and a range of other areas to support its clients managing their IT agile and efficiently.