IT Security is More than just Technology

THE ROLE OF THE CISO MOVES INTO FOCUS

www.link11.com

The Role of the CISO Moves Into Focus

Digitization promises new opportunities for the economy. Managing directors and board members of companies must now decide where the business is to develop and what the value chains of tomorrow will look like. To ensure their future viability, they will rely on new technologies, automation and intelligent production. However, as digitization progresses, enterprise value will increasingly depend on new business models based on intangible assets such as data, platforms and software applications. Today, the availability, integrity, and IT security of services and data are becoming basic prerequisites to conducting day-to-day business.

Organizational forms and role allocations face changing market conditions and requirements should therefore be scrutinized.

Safe Implementation of Digital Change

Many challenges must be mastered to plan and implement digital change safely in the truest sense of the word. One of the most important challenges involves adapting internal organizational forms and reallocating risk management roles. According to a 2019 survey from the management consultancy Rochus Mummert, about half of German companies is affected by cybercrime.[1]

When restructuring the organization, the board and management should make digital change a priority. And those responsible for digitization and IT security must be involved in strategic and business decisions right from the start.

"Ultimately, the development of business models and value chains always leads to the need for a reassessment of the internal organizational structure in order to take better account of the existing and potentially new liability risks," says Professor Dr. Thomas Grützner, Partner at Latham & Watkins and a specialist in compliance and white-collar criminal law issues. "This can often be more complex in the case of intangible assets than in the case of tangible assets, especially if no comparable empirical values or risks have been learned from the previous business models.”

60%

of organizations suffered two or more business-disrupting cyber events in the last 24 months. Ponemon Institute

Nine out of ten companies in Germany know that digital change is making them more vulnerable.[2] There is also a 76% consensus that cyber threats are a relevant operational threat. Everybody's business is being disrupted, according to a study from the Ponemon Institute.[3] Ninety-one percent of the companies surveyed worldwide have suffered at least one cyber attack that led to interruptions in business operations in the past 24 months. Furthermore, 60% reported two or more cyber attacks during this period.

Not a week goes by without a company informing the public about a security incident or data breach. The headlines and damage reports show that the interruption of operational processes, the failure of services, or the loss or manipulation of data can pose a very real existential threat. This is regularly accompanied by the question of internal responsibility, as well as external (civil or criminal) liability. Companies struggle with these changed framework conditions and often only learn from their own painful experiences, according to Grützner. This is demonstrated by incidents in recent months:

- At the beginning of March, an energy company supplying several western US states with electricity fought for 10 hours with "interruptions to the operation of electrical systems" due to DDoS attacks.

- In March 2019, the Norwegian aluminum producer Norsk Hydro had to stop all production and administrative processes worldwide because ransomware had spread throughout the company network.

- Also in March 2019, the criminal investigation department of Kempten, Germany, registered an increased number of reports from companies whose data and hard disks had been encrypted by cybercriminals in order to blackmail them. The victims included companies, doctors' offices, and car dealerships.

Why IT Security is a Full-Time Task

Nevertheless, it is astonishing that so few senior managers at companies discuss IT security and address internal cyber risks as a top priority. What's more, the number of companies that have already integrated IT security firmly into their business strategy is still too low (45%), according to EY's Global Information Security Survey 2018-19.[4]

55%

of companies do not see security as part of their corporate strategy. EY

In 60% of companies, the person responsible for IT security is not a member of the management board.[5] Companies need appropriate leadership and processes so that their digital transformation can be backed up with professional security measures. This field of activity is increasingly being assigned to a Chief Information Security Officer (CISO). This person should identify, communicate, and manage information risks. Management should also extend beyond the purely technical area to the legal department and executive board.

The CISO's field of activity is very dynamic. Key parts of their work include:

- Strategic planning and development of concepts and guidelines for IT security. In doing so, they work closely with all specialist departments and partners. Responsibility for technical implementation.
- Control and coordination of security measures.
- Continuous analysis and optimization of IT security strategies based on business processes.
- Assumption of tasks in the area of prevention (i.e., development of training measures to sensitize employees).

According to a PWC report entitled "Global State of Information Security Survey 2018",[6] 52% of the globally surveyed companies have already created the central position of CISO, and thus recognized the importance of security for their organizations. In 2006, the value was only 22%.[7]

"This development will continue with the increasing importance of a company's intangible assets and the correspondingly higher liability risks in the event of inadequate IT security," explains Grützner. "It is to be expected that the legislator and jurisdiction will also continue to act and concretize and adapt the legal framework conditions as well as the liability criteria to the rising importance of intangible assets. The GDPR is one step in this direction; the corporate compliance monitorship law, which affecs criminal offences from within the company, would be another."

Alternatively, the Chief Information Officer/CIO (27%) and middle/lower management assume responsibility for the security of communication, technologies, and data in the company. Generally, the larger the company, the more likely it is that the topic of IT security will be assigned to specialists such as a CISO. However, in reality, information security is really only a matter for the boss – that is, the CEO, hence in fact rated as a matter for the boss – in exceptional cases and in very small companies. The Global Information Security Survey 2018-2019 by Ernst & Young reports that the responsibility for IT security is primarily at the senior level.[8]

52%

of companies say that they have appointed a CISO. PWC

The CISO Must be Closer to Top Management

In the analogue world, IT played a supportive role in many companies. With digitization, it is moving to the center of entrepreneurial activity. Possible disruptions, business interruptions, and data breaches have a direct impact on the operating business and thus on key financial figures. Almost all decisions in Industry 4.0 concern IT and are therefore relevant to the work of the CISO. It is the CISO's job to identify, assess and, if possible, avert new risks.

Whether a company is introducing new products or taking over companies (M&A), the CISO role extends far beyond the selection of firewalls and virus scanners or systematic patch management. In addition to technical skills, they must increasingly think in a company-oriented manner; for example, when assessing risks when purchasing intangible assets as well as software or data. When a DAX group takes over an innovative start-up, the start-up's liability risks are transferred to the group in addition to the purchased know-how. Mistakes, omissions, or security gaps from the start-up's past can suddenly affect the group as the new owner. In the case of a data breach, fines, according to the DSGVO, can amount to up to 4 % of annual turnover, which in the case of a start-up tend to be lower than when the annual turnover of the new owner, the group, is used as the basis for assessment. Figures from the health sector show just how important the availability CISO can be when it comes to company takeovers: the consulting firm West Monroe Partners interviewed managers specialising in the conclusion of purchase agreements in the healthcare sector about their strategies and experience. 58% of respondents identified a problem in IT security after concluding the acquisition of a healthcare company.[9]

58%

of buyers of a healthcare company discovered an IT security problem in the aquired company after the transaction was completed. West Monroe Partners

Direct Reporting Line to Corporate Management

The position of the CISO, which has existed since the 1990s, led a shadowy existence for a long time. To date, there is no standard that defines the scope of this position and the associated reporting channels within the company. A CISO reports most frequently to the CIO, and thus only indirectly to the management board. This hierarchical integration can lead to conflicts of interest, as the development and operation of IT is not separated from IT security issues. Grützner points out that a company can also ask itself whether the reporting lines meet the organisational and supervisory obligations in the company in every case.

Furthermore, the CISO can find themselves subject to the CIO and the CFO's conflicting priorities. The CFO's area of responsibility is increasingly extending to areas such as digitization and IT security. This means they also control the IT budget. This means that IT security is not always seen as part of the corporate value chain. Forward-looking, cost-intensive investments in the security of IT infrastructures, data, and devices are difficult to convey from the perspective of increasing efficiency. This calls for a change in the way we think, so that IT security is not viewed as a cost factor, but rather as a differentiating factor compared to other providers and as a pioneer of digital change. In the face of increasingly intense competition, a company can use secure digital processes to build trust in the market and set itself apart from other, less-secure providers. Only 44% of companies have recognized this opportunity so far.[10] At the same time, IT security helps to minimize financial risks. Damage caused by cyber attacks can quickly far exceed the investments made in the security of infrastructure and IT landscapes.

However, a direct reporting line to the board does not yet mean that IT security is really in the hands of management and given the corresponding priority in the company. Every company must find its own form of company organization, one in which the objections of the head of security are actually listened to. "Ultimately, the specific design of governance structures will also have to be the result of a risk analysis of the company," predicts Grützner. In many cases, close cooperation with the CEO will be a good way to accomplish this. The reporting line of CISO-to-Chief Compliance Officer (CCO)- to-CEO can also create a good balance between the CIO, who is driving digital change, and the CISO, who is concerned about IT security issues.

Direct reporting channels to the management board demonstrate that IT and IT security are viewed as critical for the company. This also pays off if IT security, which is embodied by the CISO, is already taken into account in the strategic project requirements for important projects and not simply integrated into implementation questions within a current project's framework. Through consistent communication and early integration of CISOs into strategic and practical transformation, IT security is seen as a fully-fledged business process and thus anchored in the minds of corporate management. If the

44%

of executives see cyber security as a competitive advantage for their organization, while 56% view it as a cost of doing business. Cisco

CISO has the necessary scope to maneuver and is involved as a direct contact in decisions made by division heads, they can safeguard the company's security interests. In this position, they can support their company in creating holistic risk management and implementing digital transformation. This includes the protection of company information and IT technologies and thus of people (whose data is stored in the IT systems) and organs from threats.

Conclusion

The tasks of IT security and data protection are of outstanding importance for the future viability of companies. If the task is to be mastered successfully in the long term, it must be handled by a responsible person who communicates directly with top management. Companies that succeed in making IT security an integral part of their identity and corporate culture will be significantly less vulnerable than less focused organisations in these areas. And the CISO will play an important role on this journey.

Sources

[1] Rochus Mummert: Around Half of German Companies Are Affected by Cybercrime, April 2019
https://www.rochusmummert.com/downloads/news/Rund_die_H%C3%A4lfte_der_deutschen_Unternehmen_von_Cyber-Kriminalit%C3%A4t_betroffen.pdf

[2] BSI: Cyber Security Survey – Cyber Risks & Countermeasures in Companies, April 2019
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/Cyber-SicherheitsUmfrage_2018/cs_umfrage_2018_node.html1

[3] Ponemon Institute LLC: Measuring & Managing the Cyber Risks to Business Operations, December 2018
https://static.tenable.com/marketing/research-reports/Research-Report-Ponemon-Institute-Measuring_and_Managing_the_Cyber_Risks_to_Business_Operations.pdf

[4] EY: Global Information Security Survey 2018–19, October 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

[5] EY: Global Information Security Survey 2018–19, October 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

[6] PWC: The Global State of Information Security Survey 2018, November 2018
https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

[7] CIO.de: The Global State of Information Security 2006: Der Teenager im CISO-Büro, November 2006
https://www.cio.de/a/der-teenager-im-ciso-buero,829264

[8] EY: Global Information Security Survey 2018–19, October 2018
https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

[9] West Monroe Partners: Reshaping Healthcare M&A: How Competition and Technology are Changing the Game, May 2018
https://www.westmonroepartners.com/Insights/White-Papers/Healthcare-MA-Survey

[10] Cisco: Cybersecurity as a growth advantage, 2016
https://discover.cisco.com/en/us/security/whitepaper/cybersecurity

About Link11

Link11, headquartered in Germany, is a leading IT security provider that ensures business continuity. The company's patent-pending solution protects websites and IT infrastructures through its Cloud Security Platform against Distributed Denial of Service (DDoS) attacks. Additional services such as a Web Application Firewall (WAF) or a Content Delivery Network (CDN) complete the offering, ensuring 360° protection and performance for international customers. Since the company was founded in 2005, Link11 has received several awards for its innovative solution and strong growth.