Gerhard Steininger
VP Sales & Business Development
asvin GmbH, Stuttgart

Cybersecurity is an Essential Component of the M&A Due Diligence Process

Cybersecurity is increasingly a cause of significant operational and financial risks for entire companies. It urgently needs to be included in the process for mergers & acquisitions. (M&A). This is because potential threats and areas of attack for cyber criminals do not arise out of nowhere. They develop by risky neglect of cyber risks, by incorrectly emphasizing priorities and by deliberately covering up incidents or damage in the run-up to company sales. Therefore, the topic of cybersecurity should be firmly anchored in due diligence procedures.

The example of the Swabian battery manufacturer Varta shows how a serious cyber incident can have a decisive influence on the future of the company and in particular on the sale of business divisions. Varta was a restructuring case in 2024. A restructuring roadmap was drawn up to secure the company's future. It was precisely at this stage that a ransomware attack was launched on the already ailing battery manufacturer. Production was paralyzed for weeks, causing damage in the tens of millions. The costs and damage made the existing restructuring plan obsolete overnight. In addition, the financial planning systems were shut down, which simply made it impossible to produce reliable key figures and balance sheets. Last but not least, this cyber incident caused financing banks and investors to lose further confidence in the company and the crisis at Varta reached a new peak.

> *"How did you go bankrupt? Two ways: Gradually, then suddenly."*
> (Ernest Hemingway – The sun always rises)

Ransomware attacks are the most frequently occurring cybersecurity attacks. According to many experts, it is not a question of whether you will be a victim

Mirko Ross
Founder and CEO
asvin GmbH, Stuttgart

of an attack, but when! This example also shows that cybersecurity is often not yet on the CEO's agenda. According to a survey published by the digital association Bitkom at the end of August 2024, the economic damage caused by attacks on companies increased by 29 percent to 266.7 billion euros last year – a new record. Around 267 billion euros is an enormous amount of money that affected companies' needs elsewhere for healthy business development.

Cybersecurity due diligence (CSDD) is missing from the M&A agenda

In particular, companies in the M&A focus that are up for sale due to restructuring measures or rapid growth, have a fundamental problem with providing sufficient resources for cyber security and the implementation of necessary and preventive measures. Security gaps are therefore a very serious risk that is automatically transferred to the buyer. In principle, such cyber risks are not priced in and taken into account in the negotiations. However, those who incorporate cyber security issues in M&A directly into their due diligence (DD) process are clearly on the safe side. Examples of this are rare, however, because this practice has simply not been implemented to date. What is clear, however, is that billions can be saved by recognizing and eliminating attack vectors in good time.

Private equity companies, banks and consulting firms have recognized the trend and are strengthening their offering with dedicated cyber risk analysis expertise. The declared aim is to quantify the disadvantages and losses methodically in order to be able to price these in as parameters in the purchasing process and hedge them better.

Threats from cyberspace require cyber risk analysis in due diligence

Damage, loss of control and reputational damage caused by cyber attacks are very expensive for the companies under attack. Added to this is another problem:

Attackers move unnoticed in a company for an average of 151 days before the attack is detected. Enough time to extract data and prepare for the execution of ransomware. Bad for buyers' companies when risks from such undetected attacks become effective after the sale has been concluded. There is therefore an urgent need for action, especially in the case of acquisitions and mergers: There must be a fundamental reassessment of the costs on the due diligence agenda. If cybersecurity measures are not addressed and priced in, the risks increase for buyers in the M&A process by unforeseen costs due to cyber attacks after the takeover has taken place.

A "quick strike" analysis optimized for cyber risks in the due diligence process can identify problems at an early stage. It points out critical threats and prioritizes and quantifies the business-critical segments. Cyber resilience can thus be taken into account in the purchasing process.

Recognizing the added value factor through cyber security due diligence

Cyber security is becoming an indispensable factor in M&A and is generally recognized as a growth model. The fact that cyber resilience can contribute to value creation, can become a unique selling point or even a competitive factor. Companies in the USA in particular have recognized this and are playing a pioneering role here. The specific liability risks, especially for companies under SEC supervision, play a special role here. Companies under the supervision of the SEC are obliged to assess the impact of cyber attacks and formally inform the SEC within specified deadlines. Failure to do so can result in severe sanctions from the capital market regulator.

Outside the USA, the risks posed by cyber attacks are often still too much ignored or are simply accepted. The share of proactive cyber risk prevention in the IT (OT) budget is currently between 10 and 15 percent. In security-critical industries such as finance or healthcare, however, this proportion can be higher, often up to 20 percent. What should not be neglected in the cyber security market is the fallacy of lacking size. Because cyber resilience is considered difficult to demonstrate and can only be realized at high extra cost, it is assumed that only large

companies or those that are existentially dependent on resilience as operators of critical infrastructure can invest here. Although this is true in the old way of thinking, it only applies to a limited extent in the new market conditions. Today, cyber security is feasible at a manageable cost through clever risk analysis and well-balanced expenditure prioritization. At the same time, pre-set cyber security is becoming an important unique selling point.

"Cybersecurity Quick Strike Due Diligence Framework"

The following figure shows an overview of the "asvin Cybersecurity Quick Strike Due Diligence Framework". In principle, the asvin framework is divided into 4 areas.

▶ **Cybersecurity Management System:**
Current regulations often require the establishment of a CSMS (Cybersecurity Management System), which is often a quality management system specifically for cybersecurity. Core processes and their controls are described there.

▶ **Cybersecurity core processes:**
Regular testing of IT components is important for the defense against and detection of attacks. To this end, asset management data is compared with data from previously created SBOMs (SW Bills of Material) and threat intelligence is set up. This context-based risk analysis, including task prioritization, is a core function of the asvin solution. It provides the perfect overview of the current cyber threat situation.

▶ **Cybersecurity supply chain:**
Many cyber incidents in recent years have been caused by the supply chain. One of the best known is the so-called "Colonial Pipeline" attack, in which a ransomware attack caused the billing system to fail, which meant that oil supplies could no longer be guaranteed in large parts of the USA.

▶ **IT/OT security architecture:**
IT has long been exposed to the dangers of cyber attacks, but operational technology (OT), i.e. the control of industrial plants, is a relatively new focus and is

increasingly affected by cybercrime. A good security architecture is characterized, for example, by the avoidance of clustering. The assessment is implemented by the *asvin IT Tool Risk by Context*.

Cybersecurity "Quick Strike" Due Diligence Framework Fig. 1

CYBERSECURITY MANAGEMENT SYSTEM (CSMS)				
CSMS Governance				
Culture and Awareness				
CS risk management	Management of weak points	Product monitoring	Supplier security management	Incident Management

CYBERSECURITY SUPPLY CHAIN
Sales - Purchasing
Supplier chain
Corporate security
Authority reports

CYBERSECURITY CORE PROCESSES
Testing
Asset management – SBOM
Threat intelligence

IT / OT RISK BY CONTEXT™
Security architecture
IT (Information Technology)
OT (Operational Technology)

Source: asvin.io

Cybersecurity Quick Strike Approach

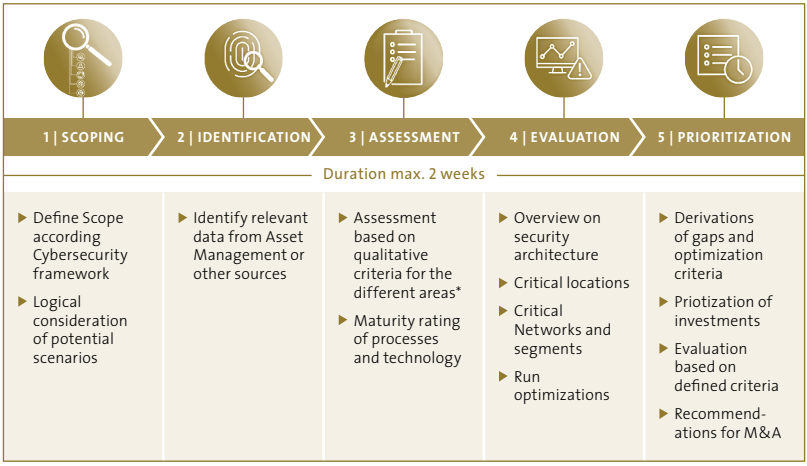
The following diagram shows the schematic procedure for a cybersecurity due diligence. The procedure is divided into 5 phases and should not take more than 2 weeks.

- **Phase 1 Scoping:**
  Based on the cybersecurity framework, the scope is defined with the relevant stakeholders.
- **Phase 2 Identification:**
  Relevant data and their respective sources are identified.
- **Phase 3 Assessment:**
  The assessment is carried out using relevant criteria.

- **Phase 4 Evaluation:**
  Here the data is put into context with the criteria. (Risk by Context) and, ideally, various scenarios are run through.

- **Phase 5 Prioritization:**
  In the final step, the existing gaps and vulnerabilities are described and at the same time, recommendations for action are derived.

Cybersecurity "Quick Strike" approach Fig. 2



** Traditional Security, Emerging Technology, Managed Security, CVSS Score, IT / OT, Threat Intelligence*

A very clear example of the need to incorporate cyber security analysis into company valuation procedures is the legal dispute that is still smoldering over the consequences of the SolarWinds hack with the so-called Sunburst Trojan. Discovered back in 2020, the incident is still one of the of the most far-reaching cyberattacks in recent times. It revealed the vulnerabilities in the security infrastructure of many large organizations worldwide. Around 18,000 companies were affected. As recently as mid-July 2024 a US federal district judge dismissed most of the claims in a lawsuit brought by the by

the US Securities and Exchange Commission (SEC) against SolarWinds. But the case revealed significant cybersecurity breaches. For example, the company was accused of defrauding investors by failing to disclose knowledge of cyber vulnerabilities in its systems before the said vulnerability that was discovered in 2020.

The SEC sued the company in 2023 on the grounds that in 2020 and prior years it had knowledge of system flaws in company statements and documents. This had jeopardized the attack that lasted almost two years(!). The US District Judge Paul Engelmayer in Manhattan ruled, however, that the disclosure after the discovery was based on hindsight and that the SEC can only pursue allegations of fraud for acts that were committed prior to the discovery of the attack.

Conclusion

The topic of cybersecurity should urgently be included in established M&A processes. Technology assessment is already a key component of company valuations today. Cybersecurity must definitely be taken into account here. According to the MIT (Massachusetts Institute of Technology), only 1 % of all cybersecurity incidents worldwide are reported today. This means that the damage caused, which according to official statistics is currently around 6 trillion dollars, is many times higher. Due diligence in M&A processes has the task of evaluating a company. Cybersecurity should therefore be an essential part of these valuations today.

g.steininger@asvin.io | m.ross@asvin.io

About the authors:

Gerhard Steininger is VP Sales & Business Development at asvin, Stuttgart, a specialist in cybersecurity management. Before joining asvin, he was, among other positions, Senior Manager at Deloitte where he also directed cybersecurity

projects at several automobile OEMs. Before that he was Director at Dassault Systems and globally responsible for MBSE (Model Based System Engineering). He holds a Master in Physics from the Ludwig-Maximilians University Munich.

***Mirko Ross** is founder and CEO of asvin GMBH, Stuttgart, a company specialized in cyber risk management. At the federal level, he uses his influence as a member of the working group "Business Protection and Cyber Security" of the Federal Association of German Industry (BDI). Here he uses his influence on statements of the association on EU regulations like Kritis decrees, NIS2 directives or the Cyber Resilience Act. At the Federal Ministry for Education and Research he is an invited expert and member of the "Strategic Platform on Digital and Industrial Technologies in HORIZON Europe".*