12 KEY STEPS

TO BECOMING A SUPPLY CHAIN CYBERSECURITY LEADER

Essential actions to effectively protect your company against cyber risks

PUBLISHED BY

BVL

transport logistic

Dear visitors of transport logistic, dear network of BVL, dear decision makers,

The digital networking of companies is growing rapidly – and with it, the threat of cyber-attacks. In a world where logistics and supply chain processes are increasingly managed digitally, cybersecurity is no longer a fringe topic but a central business challenge. To provide you with practical strategies for securing your digital infrastructure, we present the new white paper "12 Key Steps to Becoming a Supply Chain Cybersecurity Leader", published by BVL and transport logistic Munich.

secida AG and BVL, together with other partners, conducted a comprehensive study in which 150 decision-makers from supply chain management were surveyed. The insights gained from this study are directly incorporated into the white paper – with clear, actionable recommendations at the management level. This management summary also accompanies the high-level expert forum "Cybersecurity in Logistics: Safeguarding Supply Chains in a Digital Age" at transport logistic Munich on June 2, 2025, moderated by secida CEO Alpha Barry.

Our goal: to raise awareness of cybersecurity within companies, show concrete actions, and thus strengthen the digital resilience of the industry. Because only those who are prepared can successfully fend off attacks.

We wish you valuable insights while reading!

Yours sincerely,

Christoph Meyer
Managing Director,
Bundesvereinigung Logistik (BVL) e.V.

Dr. Robert Schönberger
Global Industry Lead transport logistic &
air cargo exhibitions, Messe München GmbH

12 Key Steps to becoming a Supply Chain Cybersecurity Leader

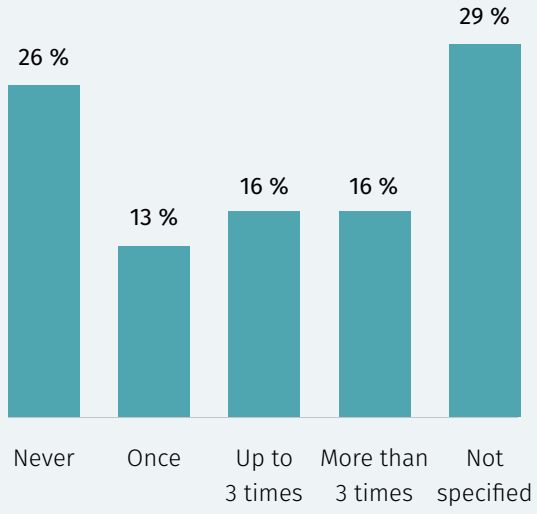
Essential actions to effectively protect your company against cyberrisks

In recent years, protection against cyberattacks has become an increasingly important topic for companies of all sizes. Today, any company can fall victim to a cyberattack, while five years ago this was still mostly a concern for large corporations. The effort to execute a cyberattack has decreased drastically, making it financially attractive for criminals to assault even small companies. Cyberattacks can lead to long operational downtimes and – in a worst-case scenario – even pose a risk to the survival of the company (as presented in Figure 1).

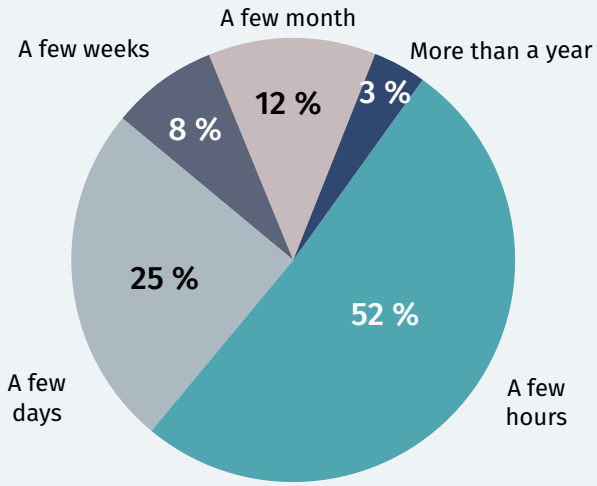
To better understand the current attitude of logistics management towards cybersecurity, secida AG, together with the German Logistics Association and other partners such as the

Figure 1: Cyberattacks in the logistic vertical – everyday crime that brings operations to a standstill

Frequency of cyberattacks in the last five years (percentage of study participants)



Time necessary to restore operations after a cyberattack (percentage of study participants)

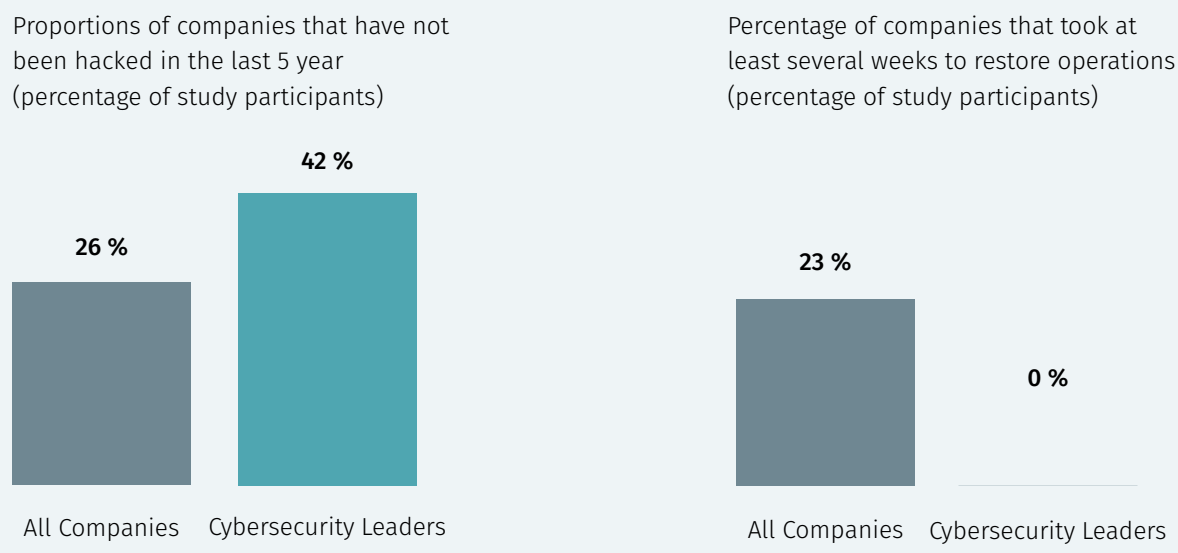


software manufacturer One Identity and the Schunck Group, conducted a study with responses from over 150 decision-makers in German logistics. In this whitepaper a cluster of companies that combine above-average economic success with significantly higher performance in cybersecurity was further analyzed: The Supply Chain Cybersecurity Leaders. The strong cybersecurity performance of the Supply Chain Cybersecurity Leaders pays off: This group of companies is hacked significantly less often than the average. In addition, they need significantly less time to recover from successful cyberattacks (see Figure 2). We have structured the results to present clear recommendations for action and measures for companies who would like to implement proven good practice.

Our study clearly shows that the good cybersecurity performance shown by the Supply Chain Cybersecurity Leaders not only has no negative impact on their economic success, but also measurably increases protection against cyberattacks. Please refer to our 2023 report for more details.

During our 2023 study, we asked participants about practices used in cybersecurity and IT infrastructure operations. Governance, processes, and technology were covered. When we compared usage frequencies of individual practices for the Supply Chain Cybersecurity Leaders with average usage frequencies across all participants, 12 specific practices stood out (presented in Figure 3).

Figure 2: Success is possible – top companies are rarely hacked and eliminate effects more quickly

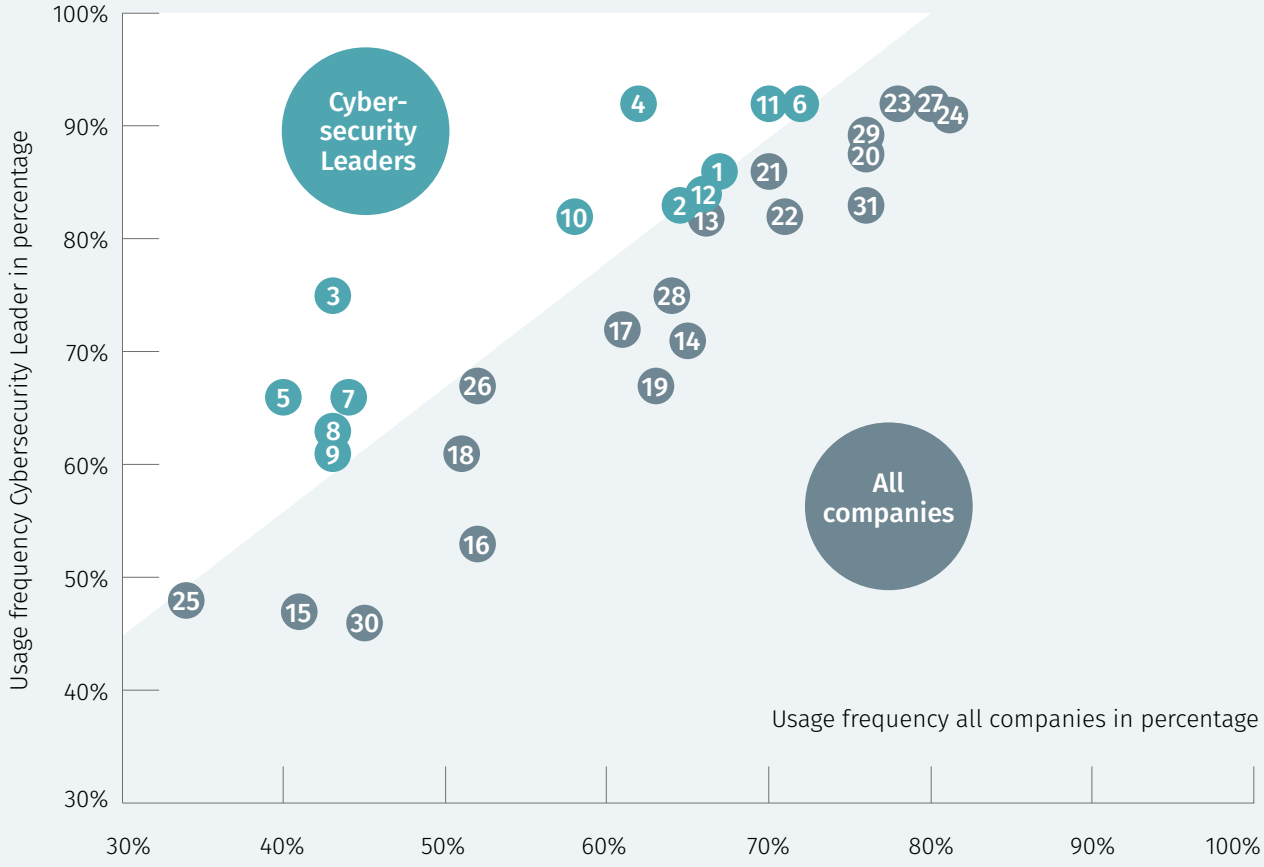


The Leaders use these practices far more frequently than other companies. Further analysis showed that this is not only statistical correlation. These practices are the potential root cause for high cybersecurity performance shown by the Supply Chain Cybersecurity Leaders.

In this white paper, we showcase those practices in more depth, as we believe that their implementation will improve the cybersecurity stance of any company. The more practices can be implemented the closer a company will potentially get to becoming a Supply Chain Cybersecurity Leader itself.

Figure 3: Usage frequency of cybersecurity and IT operations practices, comparing Supply Chain Cybersecurity Leaders to all study participants

Highlighted practices are implemented significantly more often by Cybersecurity Leaders.



1 Defined cybersecurity strategy
2 Security guidelines and rules for IT operations
3 Specific cybersecurity KPIs
4 Business Continuity Management (BCM)
5 Regular cybersecurity drills and simulation games
6 Cybersecurity awareness training
7 Cross-supply chain cybersecurity
8 Cooperation with suppliers
9 Cross-supply chain emergency plans and workflows
10 Modern IT infrastructure
11 Effective identity and access management (IAM)
12 Implemented privilege access management (PAM)
13 Information classification
14 Asset DB
15 Support via IT-service providers
16 Use of cloud
17 Secured internal material flows
18 Secured customer material flow
19 Defined Cybersecurity budget
20 Focus on management level
21 High level of IT expertise
21 IT-Emergency plan
23 IT-Solutions Access Management
24 KVP Cybersecurity
25 Use of open source
26 Tested access policies
27 Risk Management
28 Information protection
29 Cybersecurity Monitoring
30 Aligned responsibility Cybersecurity
31 Implemented Access Management

A clearly defined cybersecurity strategy

01

A clearly defined and formulated cybersecurity strategy, which is implemented by management as part of risk management, is the best possible basis for making the company cyberresilient. The central focus of cybersecurity leaders is to effectively minimize the probability that cyberattacks result in material damage to the company. To prevent this, the following key questions need to be answered:

1. **Identify crucial processes and their supporting IT systems.** Which IT systems are essential to continue business operations? All departments need to be involved in the identification process to ensure nothing is overlooked.

2. **Define necessary protection measures.** How can essential systems and processes be secured against cyberattacks? What is the current cybersecurity status, and which steps still need to be implemented?

3. **Plan for the emergency.** How will you continue business operations when essential IT systems are not available during a crisis? Who on the management team will take which role? Where will you quickly get the incident response and forensics resources you do not have on the payroll?

4. **Implement monitoring and response.** How can attacks quickly be detected and an effective response be ensured? Which systems can consistently scan for possible attacks? What are adequate measures in reaction to an alarm? Who oversees checking these alerts and implementing further (cross-supply chain) measures?

5. **Ensure optimal cyberresilience.** A good cybersecurity strategy must include measures to quickly and effectively restore operational capability (i.e., a situation as close as possible to the original state) after an attack.

Comprehensive security guidelines and rules for IT operations

02

After implementing a comprehensive cybersecurity strategy in collaboration with IT and departments, it needs to be broken down into actionable elements: corresponding guidelines and rules for running IT operations are the basis for effective implementation. To create the best possible outcome, we recommend dividing the design into four blocks:

1. **Organization.** How should the organization behave in the context of cybersecurity?
2. **Behavior.** How should employees deal with security risks?
3. **Processes.** How should company and IT work securely?
4. **Technology.** What technical measures must be in place?

It is not necessary to develop all guidelines within the company: frameworks such as ISO 27001 or NIST can serve as orientation. In addition, companies must check if they need to follow specific legal regulations (e.g. in Germany DORA for the financial industry or KRITIS for critical infrastructure).

Specific KPIs for monitoring and optimizing cybersecurity

03

In cybersecurity, as in everything, you can only optimize what you measure. That's why leading companies use key performance indicators (KPIs) to enable constant measurement and improvement of cybersecurity activities.

In the first stage, companies should focus on KPIs that measure resources and effort invested into cybersecurity. Useful KPIs for that stage are, e.g., the share of cybersecurity budgets of the total IT budget, the cybersecurity training completion rate, and the frequency and success rate of applying security patches to IT systems.

In a second stage, additional KPIs can be added that measure success of cybersecurity activities. Examples for such KPIs are the mean time to detect a cyberattack, the number of security incidents detected, or the share of IT systems and devices compliant with security policies.

Companies will also have to deal with conflict between cybersecurity targets and other IT targets. E.g., most companies will benchmark IT operations cost and try to reduce it. Increasing the intensity of cybersecurity monitoring, which increases the probability of detecting cybersecurity attacks, will increase IT operations cost. Companies will have to define the right balance between new cybersecurity targets and pre-existing IT targets.

Business Continuity Management

04

Every company knows it needs to ensure that business can continue as frictionless as possible in the event of a fire resulting in the loss of parts of the operation. Today, it is just as necessary to develop a clearly defined business continuity management plan for cyberattacks in which central questions must be answered and resulting challenges solved: Each department needs to analyze which systems and assets are essential for them to continue their business. In addition, it needs to be known if business can continue at all if these systems fail and for how long. The resulting requirements and solutions need to form a structured business continuity plan for the entire company. The plan needs to formulate concise actions for how and whether operations can continue in the event of failure of certain systems and what alternative solutions exist to ensure the best possible survival of the company. Solutions should have several back-up plans: if the first is a back-up of affected systems and they may fail only for a very short time, it needs to be asked whether quick recovery of back-up is truly possible. Should this not be the case, it could be examined whether a back-up of the entire system could be kept in a separate area. The supply chain should be included in all business continuity planning, which we will discuss in more detail in steps 07, 08 and 09.

Regular cybersecurity drills and simulation games

05

After business continuity plans are in place, it is important to develop a cross-departmental cybersecurity emergency plan and to regularly train its implementation like regular fire drills. The better prepared all employees and decision makers are, the more capable the company will be of ensuring its survival during a cyberattack.

Supply Chain Cybersecurity Leaders use regular cybersecurity drills and simulation games to practice optimal behavior in an emergency. IT teams should practice importing backups or effectively tracking down the hacker; production should practice implementing specific BCM measures in case of machine failure; management needs to train decision-making in an emergency, etc. The more routinely any department can deal with a cyberattack, the less effective the attack will be and the faster it will potentially be to restore operations.

Cybersecurity awareness training

06

Cyber-aware employees are crucial to protecting a company against cyberattacks. One wrong click can have far-reaching consequences. To minimize negative effects, mistakes that are cybersecurity-relevant must be recognized and reported as quickly as possible. It is essential to enable the entire company to recognize phishing emails, social hacks and the like: all employees' behavior, resulting actions and IT knowledge are central components of the company's cyberresilience. Cybercriminals know that emotional stress leads to wrong decisions, and use social engineering to successfully attack companies, when weaknesses in the IT systems cannot be found. They like to put victims under pressure in various ways to provoke the desired misconduct: "Click here quickly to prevent your salary from being transferred to the wrong account!" "Respond quickly, otherwise the boss will complain about you!" The more employees are aware of the methods attackers like to use and can protect themselves against them through verification and deceleration, the better protected the company is against cyberattacks.

There are various cost-effective service providers that offer web-based training at affordable prices, making cybersecurity awareness training affordable for companies of all sizes.

Cybersecurity for the entire supply chain

07

These days, protecting your own company against cyberattacks is no longer enough to ensure its survival. Larger companies that are closely integrated into a supply chain are particularly at risk from smaller companies in the chain that are less able to invest in their own cybersecurity.

The more clearly measures and responsibilities are defined, the more effectively cyberrisks can be managed. Safeguarding the supply chain has a long tradition in risk management, e.g. for production: What can be done if a particular supplier cannot deliver as agreed? How can production bottlenecks be avoided? What alternatives can be considered and how quickly can production be restarted?

Similar measures must be implemented for cyberrisk management: What can happen if a company in the supply chain is successfully hacked? What impact does this have on our company's IT and how can we protect against this? What impact does a shutdown within the supply chain have on our own operations? How does an attack on customer level affect our company and vice versa?

Responses to these and more questions should be incorporated into business continuity management and disaster recovery measures, meaning the measures to restore the state prior to an attack as quickly and closely as possible.

Cooperation with suppliers

08

In the same context it is essential to ensure how suppliers are currently dealing with cybersecurity issues. Companies need to implement common rules and guidelines for communication and action in the event of a successful attack across the entire chain.

Transparency and cooperation with suppliers are crucial for optimal cybersecurity. There must be an open and honest exchange regarding current measures against cyber-manipulation. If cybersecurity gaps are identified, they must be addressed as effectively as possible. Companies with more cybersecurity experience need to provide important suppliers with expertise and advice or alternatively have a suitable service provider in their portfolio.

Companies must be aware that effective business continuity management and good disaster recovery are only possible if important players within the supply chain are included and sensible alternatives defined.

Cross-supply chain emergency plans and workflows

09

After identifying and mitigating dependencies and risks in the supply chain, companies should develop cross-supply chain emergency plans: Who needs to be informed across companies if a cyberattack causes outages? What are effective measures to compensate for failure of certain processes and systems? How quickly can they be implemented? How can failed areas be restored and what is the maximum time available before company survival is at risk?

After developing and implementing appropriate actions in all emergency plans, cross-supply chain exercises must be held. This way, each link in the supply chain will be able to react quickly and effectively in case of emergency.

Modern IT infrastructure

10

Modern IT infrastructure is often less susceptible to attacks and better able to withstand current cyberthreats. This observation is based on several underlying root causes:

1. **Complex legacy IT infrastructure that has grown over the years is hard to protect, given its complexity.** The transformation towards a modern, hybrid IT infrastructure often includes streamlining said infrastructure and reducing complexity. This has a positive effect on cybersecurity.

2. **Modernizing IT infrastructure often goes hand in hand with re-design and stronger automation of IT operations. This in turn optimizes cyber-hygiene:** regular patching and software upgrades, good back-up management that adheres to current cybersecurity requirements and a good overview of all assets, applications and software used on them including current update status are implemented.

3. **Modernizing the IT infrastructure also allows companies to redesign the architecture with cybersecurity in mind.** Individual systems can be hardened against attacks and security architecture concepts, such as Zero Trust, can be implemented.

Effective identity and access management

11

A key element of cybersecurity is to authenticate (Is the person who wants to read and use this information who they claim to be?) and authorize (Is the person we authenticated authorized to access the information requested? What are they allowed to do with the information: read, edit, download?).

Identity and access management is the most effective way to implement these measures. The company must be able to clearly and unambiguously authenticate each identity in its IT infrastructure at any time and directly see what information it is allowed to access when, where and how. These identities do not necessarily have to be real people: software solutions, machines and systems also need to be defined as IT identities with specific access rights.

Specific cybersecurity measures for administrators and users with extensive access rights

12

In every company, there are user groups that have significantly more extensive rights and options for accessing information or are even able to make changes to IT infrastructure: administrators and users with extensive access rights.

Administrators are usually based in the IT department and responsible for maintaining and ensuring optimal performance of the IT infrastructure. To fulfill their responsibilities in the best possible way, they must be able to install updates, install new software or create new users. This requires rights that regular users do not receive for security reasons. In addition, there are users who, due to their position in the company, need to have access to sensible information that is not accessible to everyone. These include, for example, the finance department or HR managers, management or other leadership functions.

Administrators and users with extensive access rights are the most popular target for cybercriminals. If attackers manage to compromise a user account with such access rights, extensive changes to systems can be implemented, malware installed, or sensitive information stolen. It is essential for modern cybersecurity architecture to protect these sensitive accounts effectively.

Supply Chain Cybersecurity Leader often implement privileged access management (PAM) solutions to protect these accounts. PAM enables companies to monitor activities of privileged accounts, authorize planned activities up front, record all sensitive acitvities and directly abort in event of deviation. In addition, recording all administrative activities makes it possible to quickly and effectively determine which actions were carried out by attackers during a successful account takeovers enabling IT to quickly reverse and limit far-reaching negative effects.

Conclusion

The study "Cybersecurity in supply chains" and this whitepaper have shown that a group of companies – the Supply Chain Cybersecurity Leaders – have already achieved high performance in managing cybersecurity risks. However, decision makers from other companies, who now want to develop their cybersecurity might struggle with finding the best way to start.

In the long term, all measures discussed in this paper should be fully implemented. However, they can be implemented step by step based on time, budget, and resource capacity available. As shown in figure 4, we recommend starting with what can be implemented without in-depth cybersecurity expertise: regular cybersecurity training and cybersecurity exercises. Defining a cybersecurity strategy, expanding business continuity management and defining appropriate guidelines are essential for every company in today's world and should, if not yet in place, be tackled with urgency. When the above topics have been addressed, the cybersecurity proficiency of the organization will have increased and it will be easier to define the next steps: Is it more urgent to address supply chain issues after analyzing BCM and disaster recovery? Should IT systems be modernized? Does the company need to prioritize protection of administrative accounts and monitor roles and authorizations or is it more urgent to define key performance indicators?

With each topic a company addresses, it will become easier to identify and execute meaningful next steps. Companies should seek a direct dialog between IT and business departments from the outset, define the status quo together and develop a roadmap eliminating the existing gaps based on their cybersecurity strategy.

We hope that this overview has given companies good insights and approaches to help in their journey towards an optimized cybersecurity and will enable more companies to become cybersecurity leaders in the future.

Figure 4: Cybersecurity for SMEs – Many top company measures are easy to implement

Grouping of practices by relative implementability, ranging from simple to complex; selection and order of implementation should be guided by available resources.

Author:

secida

secida AG is a Germany-based IT consultancy focused on cybersecurity and digital transformation. We help companies to analyze, design, implement and manage their secure digitalization projects.

If you are interested in the entire study, a German-language version is available for download at this link: https://www.oneidentity.com/whitepaper/cybersecurity-in-supply-chains-progress-vulnerabilities-and-impressive-success-stories-german/.

Please do not hesitate to contact us at sales@secida.com if you need an English version.

secida AG
Rüttenscheider
Straße 120
45131 Essen
Tel: +49 211 3853 6647
sales@secida.com
www.secida.com

We thank the collaborators of the BVL-study "Cybersicherheit in Supply Chains" as the generated data of this study is the base for this whitepaper.

BVL

CODE FI Forschungsinstitut Cyber Defence Universität der Bundeswehr München

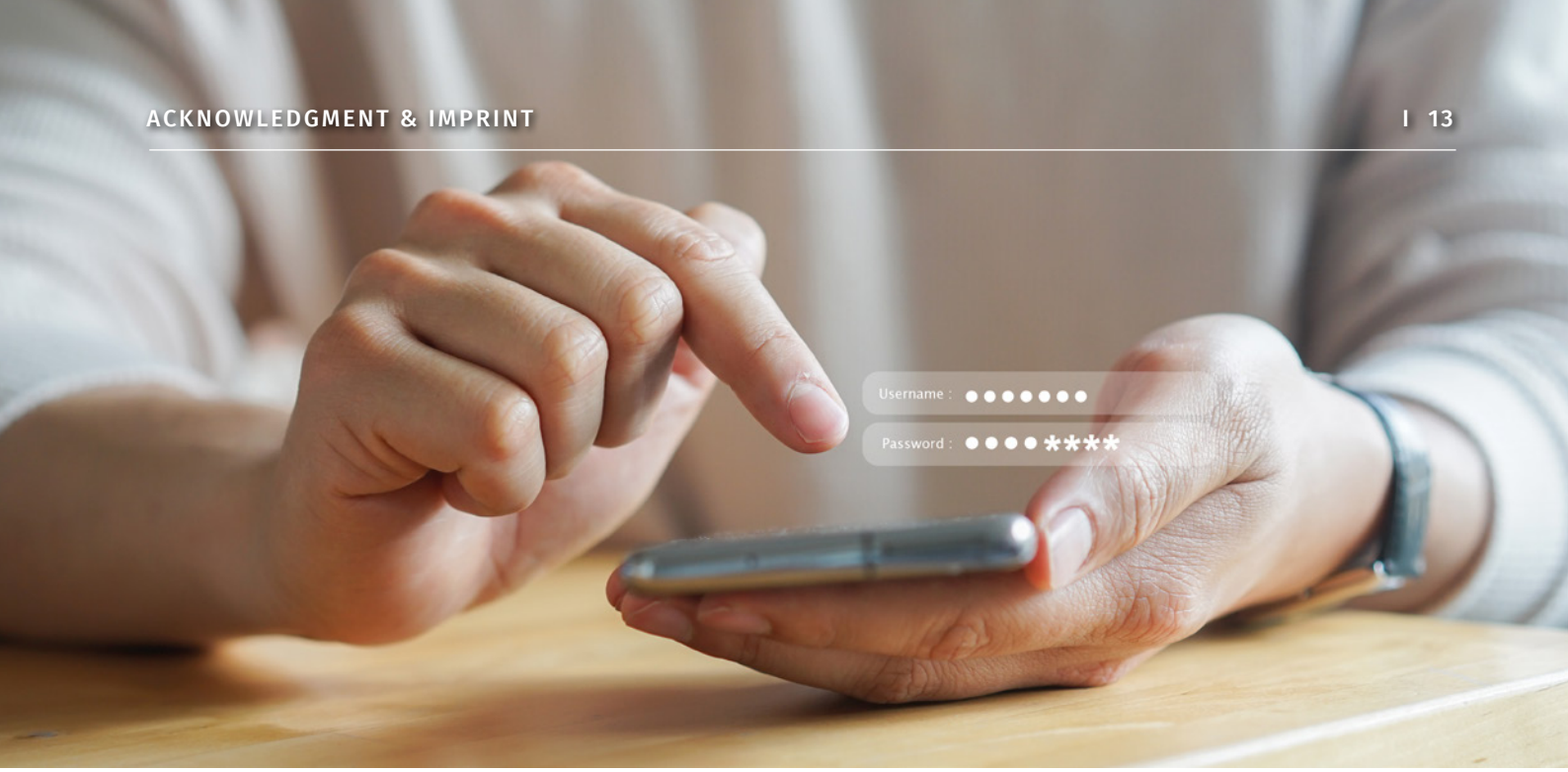
ONE IDENTITY by Quest

LEHRSTUHL PSA PRODUKTIONSSYSTEME und –AUTOMATISIERUNG

SCHUNCK GROUP

secida

Photos: stock.adobe.com: thanmano (p1), istockphoto.com: BrianAJackson (p2), champpixs (p3), tsingha25 (p4), champpixs (p6), Barriography (p7), Urupong (p10), Thapana Onphalai (p12), Chainarong Prasertthai (p13)



Published by:

transport logistic is the international trade fair for logistics, mobility, IT and supply chain management and the largest trade fair in the world for the multi-faceted transport of goods by road, rail, water and air. air cargo Europe, an exhibition of the global air cargo industry, is integrated into transport logistic.

Messe München GmbH
transport logistic
Messegelände
81823 München
www.transport-logistic.de/en

The international network of **transport logistic exhibitions** spans events across four continents. Alternating with the world's leading trade fair transport logistic in Munich, transport logistic China takes place every two years in Shanghai. In Turkey, Messe München and EKO Fair Limited organize the logitrans International Transport Logistics Exhibition annually in Istanbul. In the USA, Messe München organizes transport logistic Americas, which runs alongside air cargo Americas in collaboration with the World Trade Center Miami. Since November 2023, transport logistic Southeast Asia has also been held biennially in Singapore. The air cargo sector plays a crucial role at all trade fairs. At transport logistic in Munich, air cargo Europe is the world's largest gathering of air cargo professionals. Meanwhile, air cargo China and air cargo Southeast are integral parts of the corresponding transport logistic events in Asia. Additionally, air cargo India and air cargo Africa are independent trade fairs. Starting in 2025, both will be expanded to incorporate a multimodal approach and evolve into the transport logistic India and transport logistic Africa exhibitions.

BVL – The Supply Chain Network – The open network of BVL (Bundesvereinigung Logistik – The Supply Chain Network) brings together about 10.500 experts and leaders from several professional fields such as production, trade, service, science and politics. Its main focus is to advance the application and development of supply chain management (SCM) and logistics. BVL places particular focus on the exchange of knowledge and experience. To this purpose, it offers congresses, specialist forums and free regional group events. Highlights include the BVL Supply Chain CX and the Forum Automotive Logistics in cooperation with the German Association of the Automotive Industry. BVL is an active community whose members strive to broaden their professional horizon beyond their defined circles, thus creating effective communication in a globalized economy. As a non-profit organization, BVL acts objectively and independently without promoting any particular interests in the political or economic discourse, but strives to actively address any issues of logistics and supply chain management as a whole.

Bundesvereinigung Logistik (BVL) e.V.
Schlachte 31
28195 Bremen
www.bvl.de/en