Cyber Security Awareness: Striking the Right Balance between Quick and Reflected Response

Published in a similar form in magazine 'dhf Intralogistik', an international trade journal for internal logistics, on 8 September 2025 (7/2025)
***Author:** Stefan Riese, Department Manager Customer Service, q.beyond logineer GmbH*

The logistics industry is increasingly becoming a target for cyber criminals. Taking preventive measures against attacks is therefore no longer optional, but a necessity. However, those who focus solely on technical measures such as firewalls, end-to-end encryption or patch management are blind to what has become one of the biggest security risks in companies today: its people.

The "employee" gateway

Every day, employees access sensitive networks and thus confidential data. By presenting a false front – a supposed acquaintance, an apparently valid message or a supposedly legitimate phone call – cyber attackers are increasingly successful in their attacks. Within logistics, delivery information, customs documents, payment data and system access are particularly frequent targets. Anyone who automatically clicks, forwards or confirms without thinking can bring entire supply chains to a standstill. Phishing, social engineering and CEO fraud are no longer isolated cases, but increasingly serious everyday threats.

Technology can go a long way towards protecting company boundaries – but not the final mile. Without informed, security-conscious employees, any technical defense remains vulnerable. In order to seriously preclude crime, security awareness must be established and developed throughout the entire company. To achieve this security, companies must distinguish between two forms of response: intuitive and fast vs. logical and slow.

Fast thinking as a risk factor

Psychology shows that we make decisions on two levels. System 1 is fast, intuitive and automatic. It enables us to act efficiently in everyday life. System 2 is slower, more reflective, logical, checking for, questioning and recog-

nising pattern breaks. Cyber attackers specifically target System 1 responders. They design emails, processes or messages to appear familiar, urgent, or emotionally charged – exactly what triggers our minds into fast mode. The click is made, the caller is put through, the link is opened.

Cyber security awareness comes into play at this point, preventing cyber crime. In training courses, employees learn to take a step back at the right moment. To remain vigilant, recognise signals and pause for thought. This is a skill that can be systematically developed. A crucial caveat: cyber awareness formats should be tailored to the company, to specific risks, to observe employee behaviour and internal role distributions. Organisations can work with cyber security experts to make company- and responsibility-appropriate selections, for example one-off compulsory courses versus step-by-step awareness training. Obviously, it is advantageous if these experts can draw on experience in logistics, as is the case with q.beyond logineer GmbH.

Awareness programmes with a lasting impact

Ideally, senior management will decide against simple one-off training courses or sporadic reminders and opt for a multi-stage awareness programme tailored to the industry, the organisation and the people within it.

1. Basic training

Every first step begins with simple training courses that can be rolled out across the entire company. Topics such as password security, phishing detection and handling mobile devices are the focus at this level.

2. Risk- and role-based in-depth training

Depending on their area of responsibility, department or access level, employees should receive additional, specific training. In logistics, for example, this differentiates between responsibilities in scheduling, customs clearance or IT. In addition, employees who work from home need different content than those who work in the warehouse.

3. Individual assessments and knowledge level recording

Targeted progress is only possible if there exists an awareness of current status. Questions, tests and simulated attacks can be used to identify blind spots as well as which training courses the organisation should prioritise.

4. Integrating the current threat situation

Awareness is not a static topic. Companies should regularly update content: new scams, changed communication channels or targeted campaigns require real time scenarios.

5. Make awareness part of the culture

Awareness does not end with the last training module. It requires regular updates, reminders, campaigns and contact people. In a best-case scenario, this leads to a corporate culture in which follow-up questions, vigilance and reporting are a matter of course.

Less risk, more responsiveness

A well-designed awareness programme not only reduces the risk of human error – it also strengthens the security climate within the company. Employees feel involved and prepared, not lectured. Managers receive reliable data on the risk situation. In an emergency, the response is not knee-jerk actionism but internalised, practiced awareness. Companies benefit on many levels:

- Reduced vulnerability due to less misguided actions
- Stronger security culture across all hierarchical levels
- Faster response in an emergency thanks to trained employees
- Verifiable measures for audits and customer requirements
- Greater awareness throughout the entire supply chain.

Stay alert – before others are alerted

Technical protective measures are essential. But they fall short if the human factor is not taken into account. Especially in logistics, where processes are fast-paced, data-intensive and often cross-location, more than firewalls and encryption are needed.

Cyber security awareness is not an add-on. It is the active part of IT security that everyone contributes to – from the warehouse to the boardroom. Those who set up well-thought-out training courses continuously improve them and tailor them to real dangers not only gain security. In the end, the company can count on a team that acts appropriately when it matters most.

Stefan Riese

Stefan Riese has been supporting q.beyond logineer GmbH as Department Manager Customer Service since 2021. Thanks to his many years of experience, he knows which training courses promote cyber security awareness in different logistics companies.

Do you have any questions for logineer? Or would you like a consultation?

Write to us and tell us about your requirements if you are looking for a committed partner to help you tackle the requirements of the future with digitalisation. We are ready for the challenge. Please contact us!
https://www.logineer.com/en/contact