Threema.

Cybersecurity Study

Communication Tools:

IT Managers Caught in a Web of Contradictions

FORRESTER®
WAVE
LEADER 2024
Secure
Communications
Solutions

Threema has been recognized as a leader in secure communications solutions for companies by Forrester.

Introduction

In the business context, communication channels such as email, collaboration tools, and messaging apps complement each other seamlessly. The latter are clearly on the rise, and there are several reasons for this: our smartphones are always at hand, the technology is intuitive and less risky than email (keyword: spoofing), and chat apps are compatible with practically all data formats and enable real-time communication.

Nevertheless, irrespective of the platform in question, digital communication in a professional environment is not devoid of risks – quite the opposite, in fact. According to Europol's most recent Internet Organized Crime Threat Assessment (IOCTA)[1], cybercrime is becoming more aggressive and confrontational. At the same time, the German Federal Office for Information Security (BSI) describes a "threat situation that continues to evolve rapidly" and points to the fact that ransomware is being used more frequently against small- and medium-sized enterprises (SMEs) and public institutions.[2]

Worrying trends in terms of cyber incidents are continuously posing new organizational and financial challenges for companies. Among other things, our study shows that companies are aware of both the escalating threat potential and the legal foundation for safeguarding data. A cyberattack could quickly result in significant financial consequences, catastrophic damage to an organization's reputation, and government sanctions. Security and data protection are therefore a top priority for many companies, and, as a result, investments in IT security are being allocated accordingly. This means that German companies are doing well overall when it comes to cybersecurity.

Nevertheless, there are still cracks in the foundation, in particular with regard to communication channels. The study reveals that personal data and sensitive and confidential company data are not sufficiently protected. For example, roughly 70% of the companies surveyed claim to prohibit the use of private messengers for business purposes; however, 50% of them also assume that their employees are using private chat software alongside "official" communication channels, even though these companies are aware that most private messengers do not adhere to data protection rules and fail to protect users' privacy. This inconsistency is not an isolated occurrence. Our study reveals a whole host of contradicting statements about the implementation of cybersecurity policies in companies and highlights potential areas of improvement.

Enjoy reading!

[1] https://europol.europa.eu/crime-areas/cybercrime

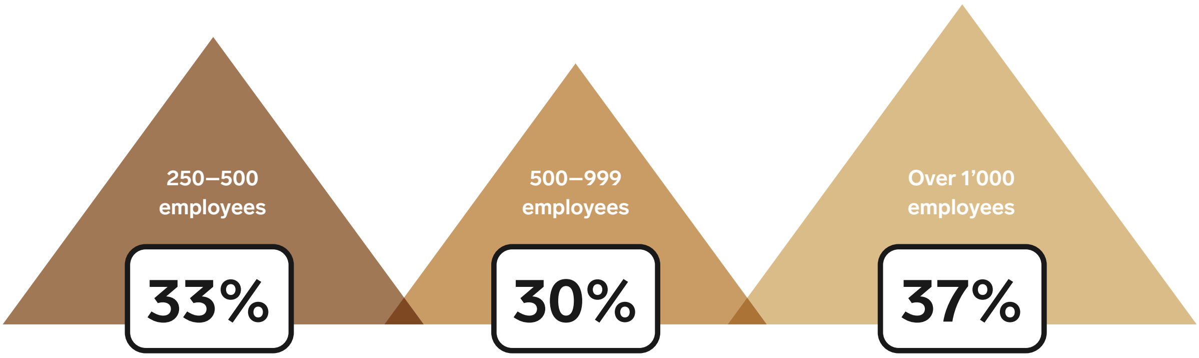
[2] https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

Contents

Background

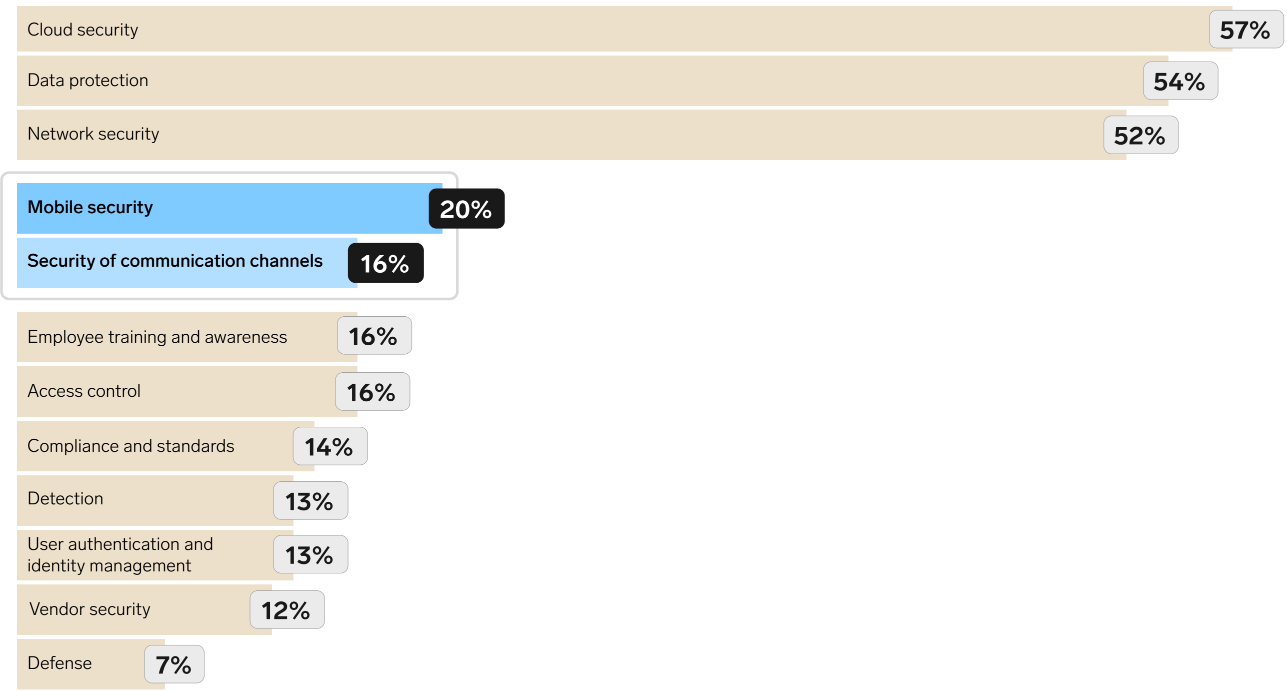
This study is based on a survey of 100 decision-makers and managers (42% in CTO/CIO/CISO roles) at companies in Germany with at least 250 employees. A total of 60% of participants identify themselves as operators of critical infrastructures. Executives from nine different business sectors participated in the study. The online survey was conducted by Arlington Research on behalf of Threema in March 2024. The aim of the study was to assess the current situation of cybersecurity in companies with a focus on communication tools and mobile devices. The findings of the study have been summarized by Threema in this whitepaper.

Sizes of the companies that participated in the study:



1. Mobile Security Is Secondary

What is currently the focus of your company's cybersecurity strategy?



More than half of the companies surveyed prioritize cloud security (57%), data protection (54%), and network security (52%) measures. The security of mobile devices ranks fourth, although only one-fifth of respondents (20%) consider it a priority. The security of communication channels (16%) is considered even less important.

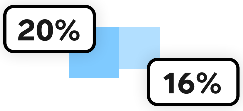
CONTEXT

Communication channels (e.g., collaboration tools, email, and messengers) play an essential role in companies' day-to-day business: they allow for a dynamic flow of information and rapid exchange of sensitive data (e.g., contracts) for both internal and external communication. Furthermore, the unstoppable advance of smartphones in companies reflects an increase in the use of messaging apps for corporate communication – a trend that continues to accelerate.

89%

consider the protection of communication channels to be a crucial component of a successful cybersecurity strategy (see Section 5).

Only one-fifth of respondents consider mobile security to be a priority.



Less than one-fifth of the companies surveyed prioritize the protection of their communication channels.

CONCLUSION

As digitalization progresses, the volume of data processed continues to grow exponentially. The downside of this development is a greater risk of cyberattacks, and data protection requirements in companies are also increasing. Companies have been subject to the General Data Protection Regulation (GDPR) since 2018 (see Section 2) and are required to implement suitable measures. The study shows that despite their awareness of these obligations, companies fail to consistently meet them.

One positive aspect is that in addition to data protection, cloud and network security are clearly a top concern: more than half of the companies surveyed prioritize these three factors. Nevertheless, areas such as communication channels appear to be neglected. Less than one-fifth (16%) of respondents prioritize the protection of communication channels, and mobile security (keyword: smartphones) is also sidelined at just 20%. It is worth noting that the vast majority of the companies surveyed (89%, see Section 5) believe that the security of communication channels is a crucial component of a successful cybersecurity strategy.

GOOD TO KNOW

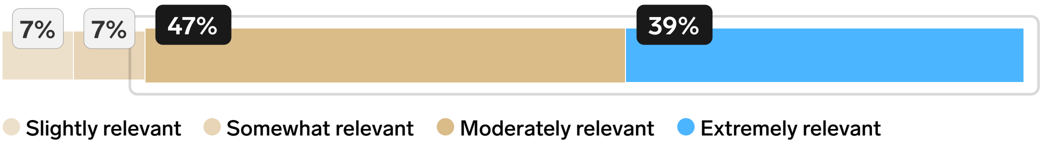
Messenger apps: Just because a product calls itself “secure” doesn’t mean it actually is. This is also true of messenger apps. Furthermore, it is important to differentiate between data protection and security. Most widely used messenger apps employ end-to-end encryption (E2EE) to protect message content. This guarantees that only the sender and the recipient can decrypt and read the message. Nevertheless, even with end-to-end encryption, it is still possible for metadata to be recorded, collected, and exploited for advertising and marketing purposes. The metadata obtained by messengers like WhatsApp, for example, includes details such as location information, the time and duration of the communication, members of a chat group, phone numbers, and IP addresses.

Collaboration tools: Although these platforms are innovative, they should be carefully reviewed in terms of security. For example, messages are not always automatically encrypted. With more than 270 million users worldwide, Microsoft Teams is one of the most popular collaboration tools. Unfortunately, its massive popularity also makes it a common point of entry for hackers to “smuggle in” malware via attachments in chats and groups. Once the malicious file has been opened, cybercriminals can take control of an employee’s computer and paralyze entire IT systems. Despite security precautions, situations like this can never be ruled out entirely. This is why having an emergency communication system installed in advance is a crucial factor when it comes to increasing a company’s cyber resilience (see Section 6). Furthermore, communication tools that lack end-to-end encryption and a “privacy-by-design” approach are not suitable for sensitive (let alone confidential) communication.

Email: Email remains an essential communication channel; however, emails are frequently unencrypted and/or difficult to encrypt. In addition, although it continues to be one of the most important and widely used communication channels, email is increasingly being replaced by instant messaging, particularly when it comes to mobile communication.

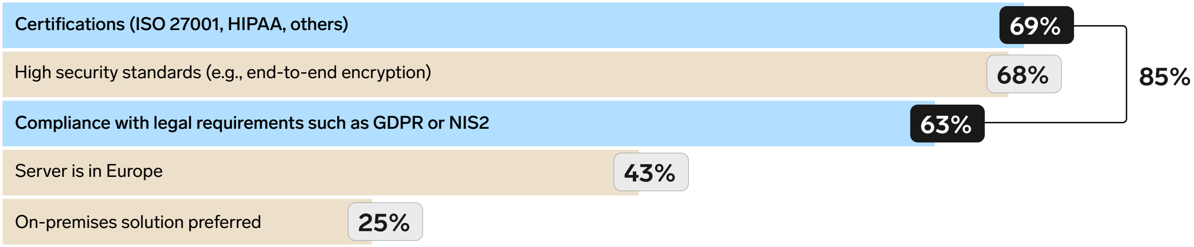
2. Inconsistent Implementation of Data Protection Measures

Is the GDPR still relevant for your company?



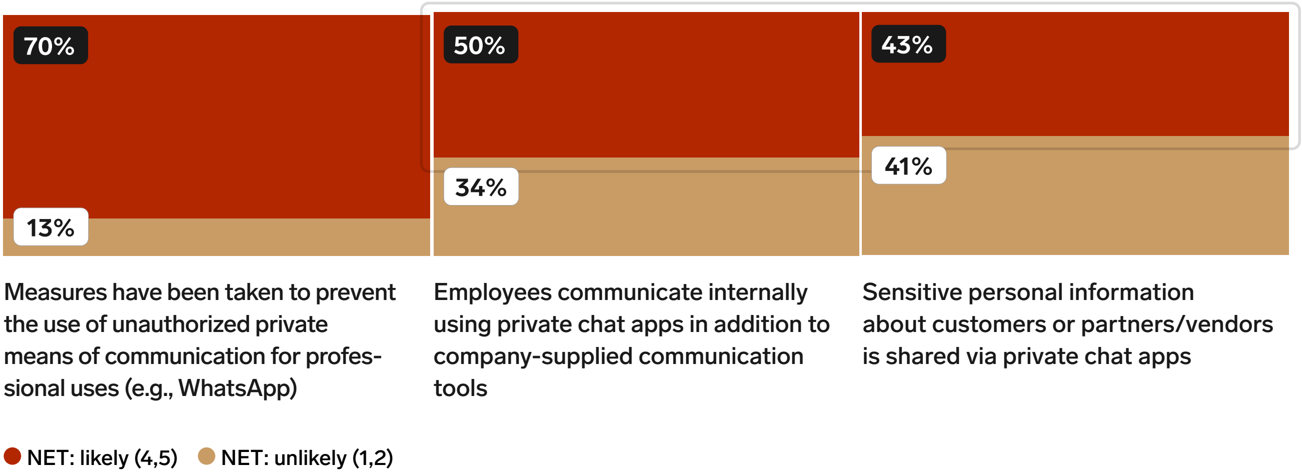
Several years after entering into force, the GDPR remains moderately (47%) or extremely (39%) relevant for companies. This can be attributed, at least in part, to the fact that data protection is a primary concern in terms of companies' cybersecurity strategies (54%, see the chart in Section 1).

Which of the following criteria do you consider when procuring communication or collaboration tools?



The acquisition of communication or collaboration tools appears to follow a similar logic: 85% of the companies surveyed consider certification (69%) and/or GDPR compliance (63%) to be key criteria.

As far as you are aware, how likely are the following to be occurring in your company?



Although they are aware of and prioritize data protection, 50% of the companies surveyed acknowledge the usage of private messengers alongside the "official" channels. In fact, 43% assume that sensitive information is being exchanged over these channels, despite the fact that management and IT managers are aware that standard chat apps are not suitable for this type of communication (see Section 5).

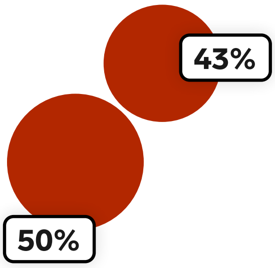
CONTEXT

The General Data Protection Regulation (GDPR) aims to harmonize data protection throughout Europe and to establish uniform data protection standards for all EU member states. The regulation went into effect on May 25, 2018, and obligates companies to comprehensively protect consumer data.

The GDPR applies to all companies that are located within the EU. This also includes all companies that are headquartered outside of the EU but have subsidiaries in the EU and/or process the personal data of EU citizens. If a company fails to adhere to the GDPR, the regulatory authority can impose fines of up to €20 million or four percent of the company's global annual revenue.

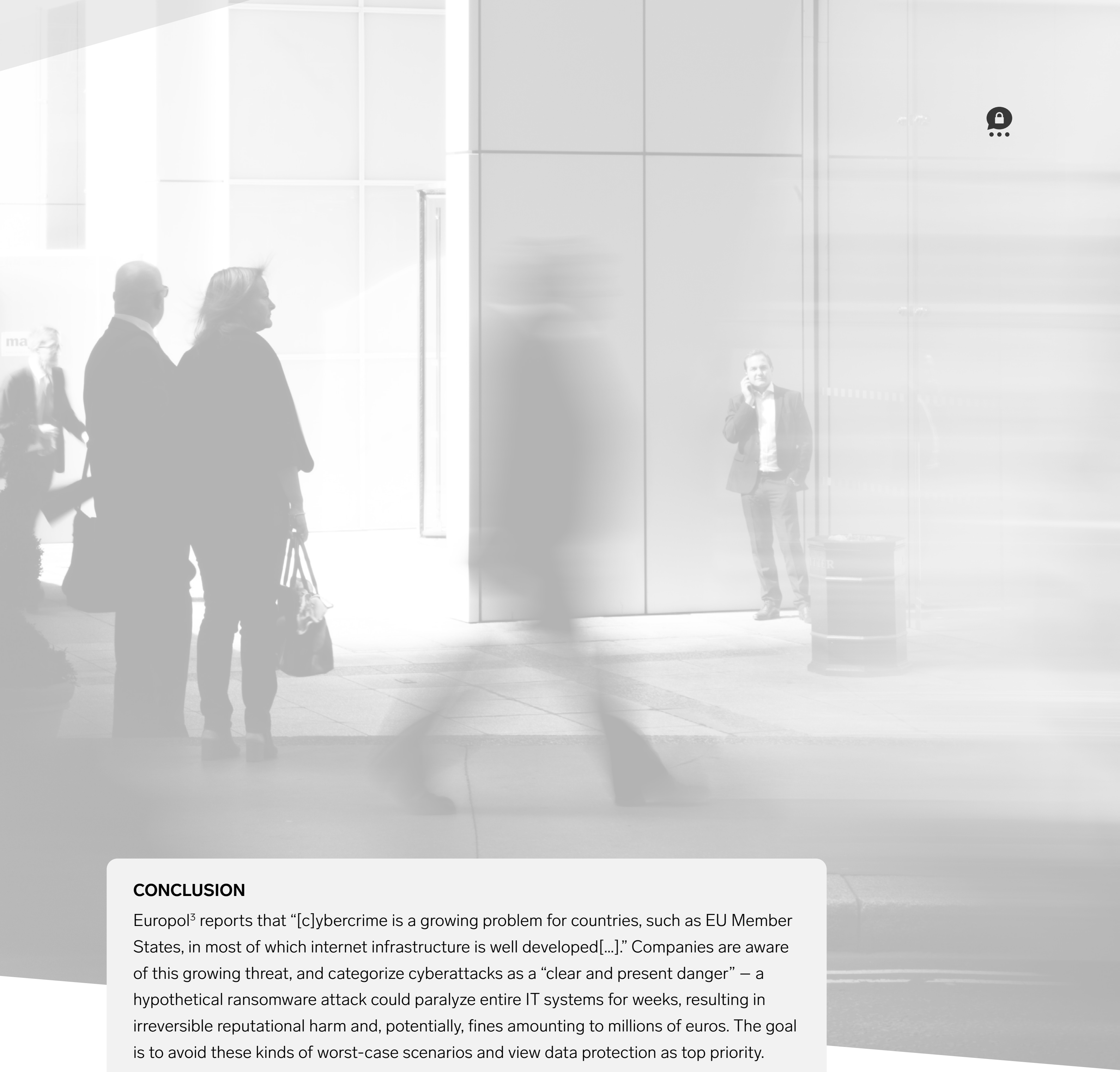
86%

The GDPR remains relevant for 86% of companies.



assume that employees are exchanging sensitive information about customers, partners, and suppliers via chat apps that are not GDPR-compliant.

believe that employees are using private messengers at work in addition to "official" communication channels.



CONCLUSION

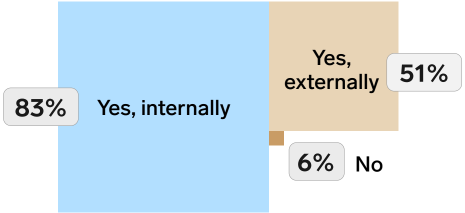
Europol[3] reports that “[c]ybercrime is a growing problem for countries, such as EU Member States, in most of which internet infrastructure is well developed[…].” Companies are aware of this growing threat, and categorize cyberattacks as a “clear and present danger” – a hypothetical ransomware attack could paralyze entire IT systems for weeks, resulting in irreversible reputational harm and, potentially, fines amounting to millions of euros. The goal is to avoid these kinds of worst-case scenarios and view data protection as top priority. As a result, it is hardly surprising that this topic remains at the top of the agenda at board meetings today, years after the GDPR entered into effect.

In reality, data protection awareness is not reflected equally in all areas. While 70% of companies claim that they prohibit the use of private messenger apps for work purposes, half (50%) of them assume that their employees are using private messenger apps at work in addition to the “official” communication channels. Only one-third (34%) believe this to be unlikely. A full 43% even think it is likely that sensitive information is also being exchanged via private chat apps.

[3] https://europol.europa.eu/crime-areas/cybercrime

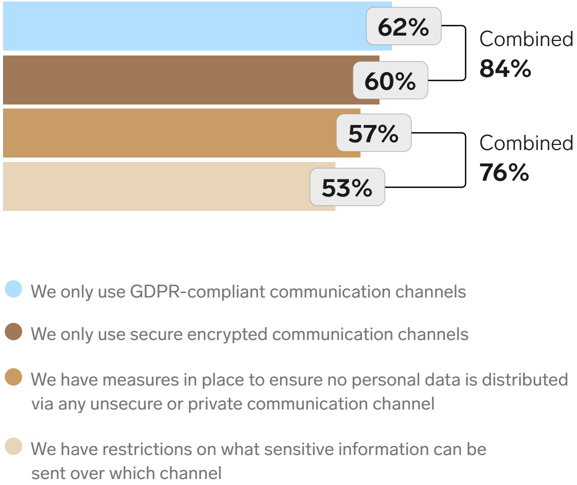
3. Private Chat Apps Tolerated as a Security Risk

Does your company exchange particularly sensitive (i.e., personal) information either internally or externally?

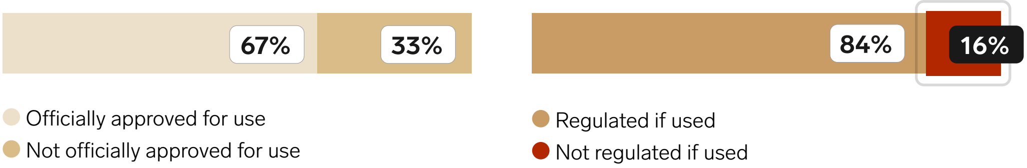


Nearly all companies (94%) regularly exchange sensitive data; the vast majority (84%) solely use GDPR-compliant and/or securely encrypted communication channels to do so. Three-quarters (76%) have either established clear standards for the exchange of sensitive data and the communication channels approved for this purpose (53%) or otherwise ensure that this data is not exchanged via insecure/private channels (57%).

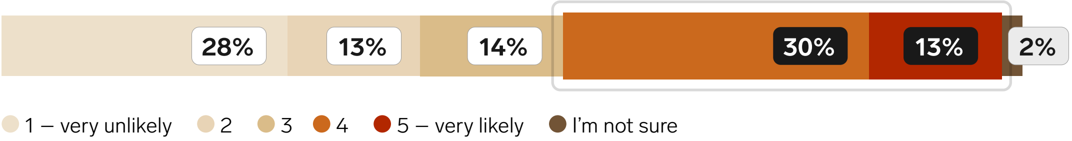
Which of the following describe your company's policy for the sharing of sensitive information?



How would you describe the use of private messaging apps in your company?



As far as you are aware, how likely is it that sensitive personal information about customers or partners/vendors is shared via private chat apps?



Two-thirds (67%) of the companies surveyed allow the use of private (non-secure) messenger apps. In most cases (84%), their use is regulated; however, this does not belie the fact that private messenger apps do not meet the security standard for corporate communication and are not GDPR-compliant.

In 16% of companies, the use of private chat apps is entirely unregulated, and 43% assume that it is likely that their employees are exchanging sensitive data via private messengers (see Conclusion in Section 2).

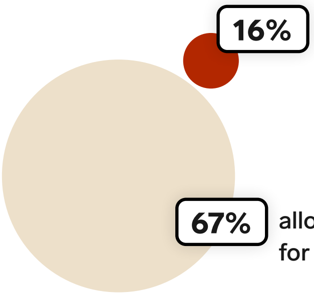
CONTEXT

The provisions of the European General Data Protection Regulation (GDPR) govern the processing of sensitive data. Sensitive personal data is protected under EU law and can only be processed if certain protections are in place. Data linked to religion, politics, and health, as well as biometric and genetic information are considered sensitive under EU data protection laws and are granted special protections. Strictly speaking, the processing of this information is prohibited.

Nevertheless, there are situations in which the processing of confidential information is allowed. Examples include when an individual has given explicit consent for their data to be processed, in order to safeguard the individual's vital interests, for the purposes of medical intervention, or if it is deemed necessary for the sake of the public interest. In general, the principle of data economy (as little as possible) governs the processing of personal information. Furthermore, all personal data is to be processed for a specific purpose; additional processing is only permitted to a very limited extent.

84%

use either GDPR-compliant or securely encrypted communication channels to exchange sensitive (i.e., personal) data.

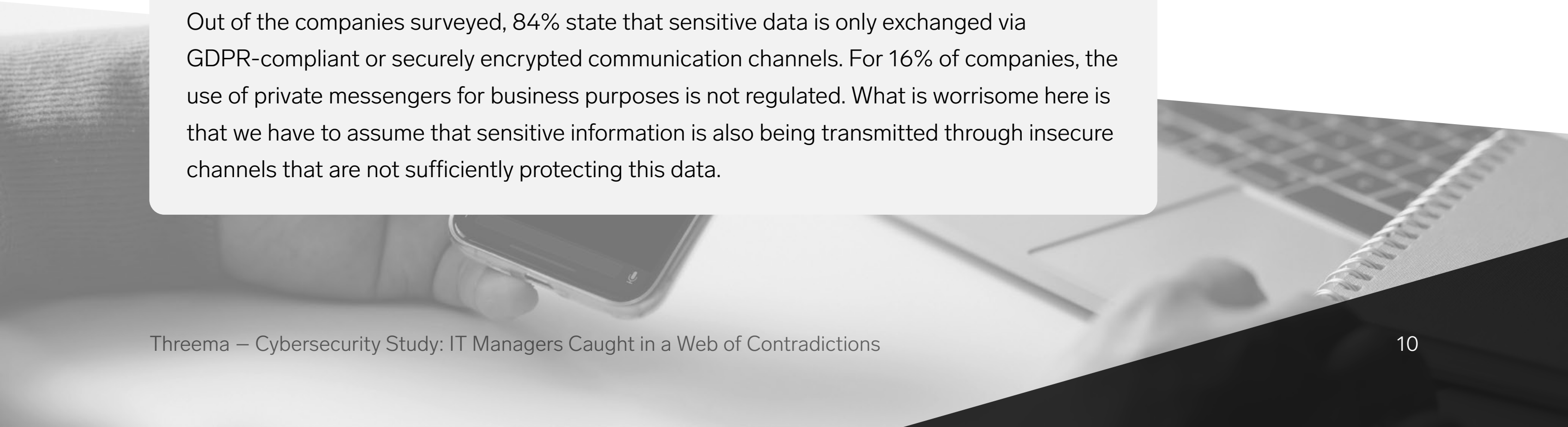


16% **state that the use of private messenger apps is not regulated in their company.**

67% **allow the use of private chat apps for business communication.**

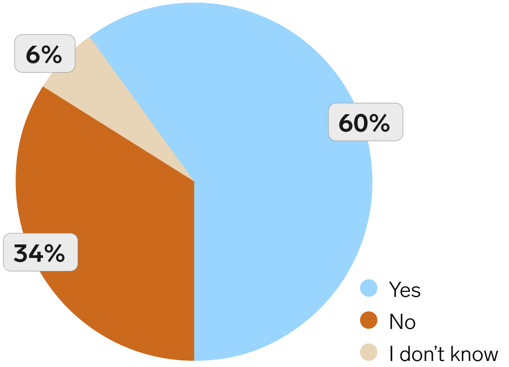
CONCLUSION

Out of the companies surveyed, 84% state that sensitive data is only exchanged via GDPR-compliant or securely encrypted communication channels. For 16% of companies, the use of private messengers for business purposes is not regulated. What is worrisome here is that we have to assume that sensitive information is also being transmitted through insecure channels that are not sufficiently protecting this data.

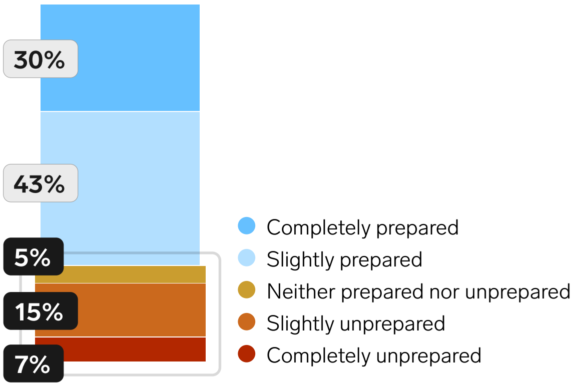


4. Many Companies Are not Prepared for NIS2

Is your company part of the critical infrastructure according to NIS2?



How prepared is your company to comply with the new NIS2 regulations currently?



A total of 60% of the companies surveyed are critical infrastructure operators, meaning they are subject to the NIS2 directive, which goes into effect on October 18, 2024. Almost three-quarters of the affected companies (73%) say they are fully (30%) or somewhat (43%) prepared for this. More than one-quarter (27%) are unprepared.

CONTEXT

The Network and Information Security Directive or NIS2 directive[4] aims to improve the security of network and information systems in the EU. Under the directive, operators of critical infrastructure and essential services are obligated to implement appropriate security measures and report incidents to the authorities.

NIS2 applies to all organizations that offer essential or important services to the European economy and society, including companies and suppliers. This includes sectors such as energy, transportation, finance, public administration, and digital infrastructure. In Germany, it is estimated that around 30,000 companies are subject to the NIS2 directive. It was approved in December 2022 and went into effect in January 2023.

The NIS2 directive becomes national law in EU member states on October 17, 2024. All affected companies must meet its requirements as of this date. These include the need for a secure communication channel in the event of a crisis (e.g., when other communication systems are non-operational). You can read more about the new directive in our whitepaper "The Importance of a Secure Business Communication Channel in View of the NIS2, DORA, and CER Regulations."

[4] https://eur-lex.europa.eu/eli/dir/2022/2555

73%

Nearly three-quarters of companies in critical sectors are prepared for the NIS2 regulations.

27%

More than one-quarter of companies do not appear to be prepared for the directive.

CONCLUSION

Starting in October 2024, the NIS2 directive will be legally binding at the national level in all EU member states. As the scope of critical infrastructures expands into new sectors, the requirements for cybersecurity will increase significantly.

The majority of companies subject to this directive (73%) say they are ready for it. What managers mean by "somewhat prepared" (43%) is unclear; their responsibilities include ensuring that suitable measures for compliance with the NIS2 directive have been implemented, that IT systems are reviewed in terms of security risks, and that employees and managers have been trained accordingly. The challenges are enormous, and questions of liability can have a direct impact on management. Particularly worrying is the fact that more than a quarter (27%) of companies are unprepared for the NIS2 directive.

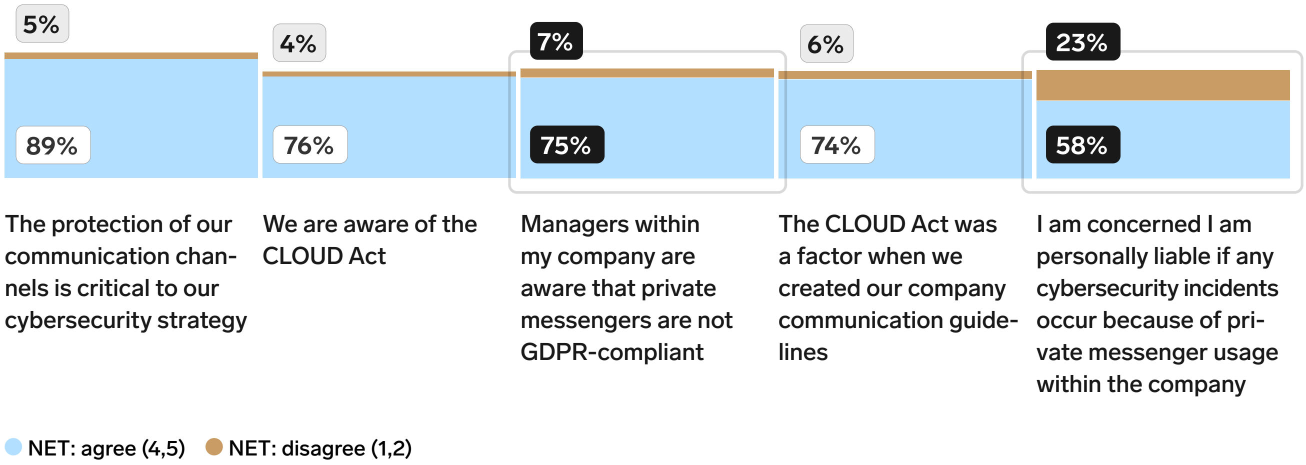
GOOD TO KNOW

NIS2 defines essential entities as large corporations that operate in one of the following critical sectors: energy, transport, finance, public administration, health, aerospace, water supply, and digital infrastructure. Trust service providers, DNS service providers, and public electronic communication network operators are also affected. The size threshold varies by sector but is generally 250 employees, an annual turnover of €50 million, or a balance sheet total of €43 million.

Important entities under NIS2 include postal and courier services, digital services (e.g., search engines, online marketplaces, cloud services, and social networks) as well as companies that are active in waste management, the food sector, the chemicals sector, industry (including mechanical engineering, vehicle construction, and development of data processing devices), and research. The size threshold varies by sector but it is typically 50 employees, an annual turnover of €10 million, or a balance sheet total of €10 million. In order to maintain communications during a crisis, companies need a secure communication channel, such as a specialized business messenger.

5. The Responsibility of IT Departments and Management

To what extent do you agree or disagree with the following statements?



Managers in three-quarters of the companies surveyed are aware that private messaging apps do not comply with GDPR. They are also familiar with the CLOUD Act, which has also influenced corporate communication policies accordingly. However, personal liability in connection with cyber incidents caused by the use of private chat apps remains a problem: over half of the respondents (58%) are worried about this type of scenario.

CONTEXT

If messaging apps that fall under the jurisdiction of the Clarifying Lawful Overseas Use of Data or CLOUD Act are used (e.g., WhatsApp or Signal), it is possible for sensitive data to be viewed or processed by US authorities at any time.

For organizations operating within the EU (see Context in Section 2), this would result in a breach of the European Union's General Data Protection Regulation (GDPR). Cybersecurity is a major concern at the executive level: with the implementation of NIS2, managers can also be held liable for any breaches of the directive. Management is obligated to authorize and monitor the proper implementation of risk management measures in the area of cybersecurity. Article 20 of the NIS2 directive states that managers must actively participate in cybersecurity training and regularly offer this training to all employees. If these requirements are not met, the managing directors will be held personally liable to the company for any damages incurred, and in the case of essential entities, individuals may be prohibited from carrying out managerial duties at the management or board level. The use of non-GDPR-compliant messaging apps for corporate communications can therefore not only result in devastating reputational damage and hefty fines, but also personal liability.

58% are worried about potential personal liability regarding the use of private messaging apps within the company.

76% are familiar with the CLOUD Act.

75% of managers are aware that private messaging apps are not GDPR-compliant.

CONCLUSION

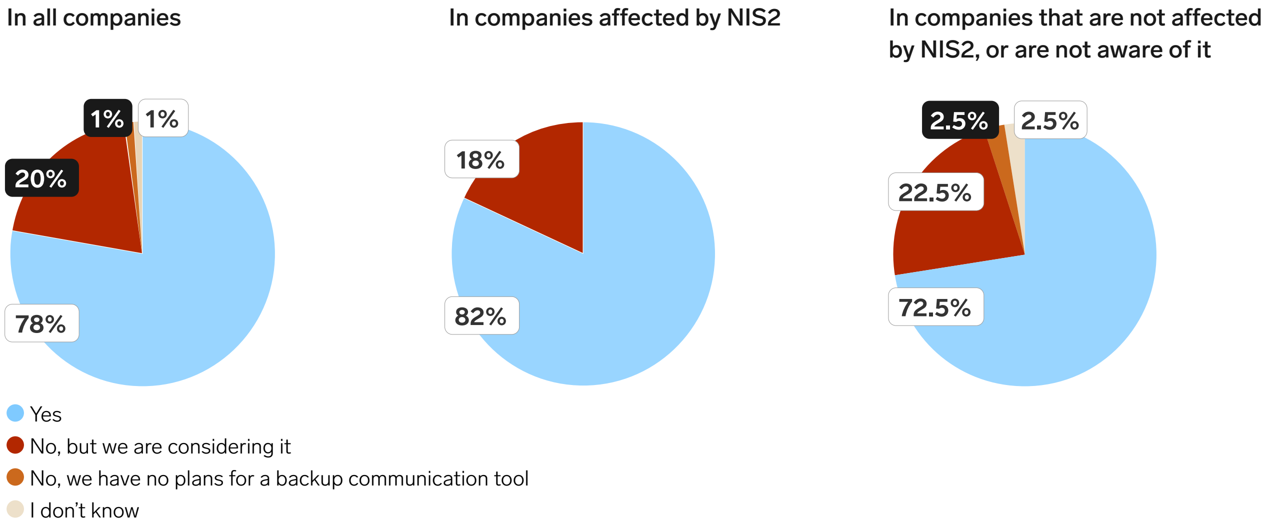
IT managers and management are aware of their personal liability, yet they are not really fulfilling their obligations. They know that private messaging apps fail to meet the requirements for business communication. Nevertheless, their use is extremely common: 50% of the companies surveyed believe their employees use insecure private messaging apps in addition to "official" communication channels. Only one-third (33%) of respondents explicitly prohibit the use of private apps for work purposes (see Section 3).

Conversely, this means that two-thirds (67%) of companies allow or at least tolerate the use of private messaging apps. In this regard, end-to-end encryption and company guidelines on security settings are often used to argue that data protection is taken seriously; however, most private messaging applications are subject to the CLOUD Act, which directly contradicts the GDPR.

In short, private messaging apps do not conform to the security standard for corporate communication and are also not GDPR-compliant. Many companies appear to be aware of the significant security and data protection risks involved, as demonstrated by the fact that managers express worry about personal liability (58%, see chart). As long as companies fail to offer their employees a secure alternative, such as a dedicated business messenger, they run the risk of corporate communication occurring on insecure and non-GDPR-compliant channels. We remain hopeful that the 23% of respondents who are not worried about this issue already have a GDPR-compliant business messenger in place.

6. No Out-of-Band Communication Channel for Emergencies

Does your company have a backup communication tool in the event of an IT system failure?



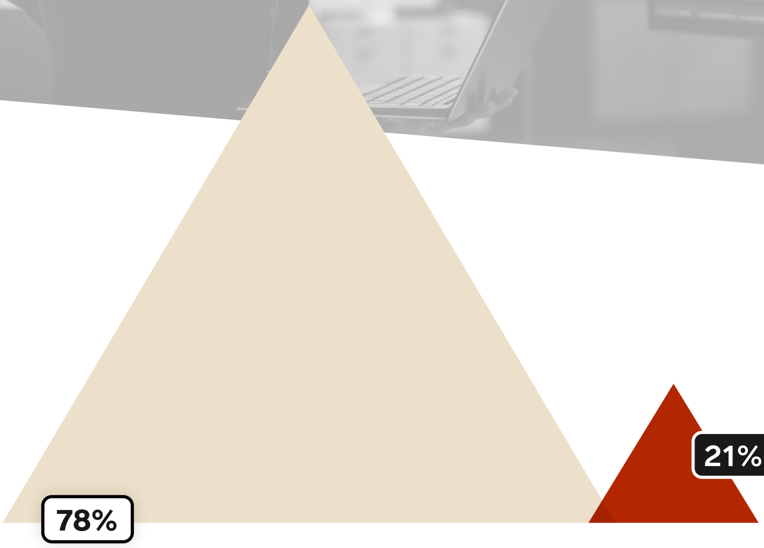
More than three-quarters (78%) of the companies surveyed have a backup communication channel in the event that the IT system and, consequently, the normal communication channels suddenly fail. Companies in critical sectors are slightly better prepared for this emergency situation (82%) than those that are not a part of the critical infrastructure (72.5%). Conversely, this means that around 20% still do not have an out-of-band communication channel in place.

CONTEXT

In the event of a cyberattack, companies must anticipate a (hopefully temporary) IT system failure. It is then up to the experts to identify the root cause of the problem and stabilize the IT system. During this time, normal communication channels (e.g., email or collaboration tools) are likely to be unavailable or infected.

This is when business continuity is vital: Disrupted business operations must be reorganized as quickly as possible, and effective communication is critical, particularly in times of crisis. A dedicated business messenger enables companies to keep important lines of communication with management, IT experts, consultants, employees, security officials, legal teams, and other stakeholders open via smartphone, even during cyber incidents.

Furthermore, a secure business messenger allows companies to mitigate potential damage: communicating via this messenger during emergencies avoids the use of potentially compromised email accounts. Furthermore, pre-defined distribution lists for emergencies allow entire departments to be reached via end-to-end encrypted group chats.



do not have an emergency communication system in place despite NIS2.

of the companies surveyed have an alternative communication solution in place in the event that their normal IT systems are not available.

CONCLUSION

It is reassuring that the majority of companies (78%) currently have a communication solution for emergencies in place.

Surprisingly, one-fifth are still thinking about it (20%) or are not even considering implementing this kind of solution (1%), even if the legal framework offers little room for doubt: as the NIS2 directive goes into effect (see Context in Section 4), companies are obligated to ensure business continuity during cyber incidents and must also have a secure emergency communication channel in place. A total of 27.5% of the companies that are not part of the critical infrastructure lack an out-of-band communication tool in case of emergencies.

In addition to the mandatory legal requirements, it is crucial to configure the emergency communication system in advance: should an emergency occur, having a configured business messenger already in place will reduce the response time and simplify crisis management.

Conclusion

Today's world of work is characterized by a continuously growing exchange of information. Communication between employees, suppliers, and customers on digital channels simplifies collaboration and streamlines processes. The role of smartphones should not be underestimated; the use of messaging apps for corporate communication has become the norm.

Mobile Security and Communication Tools

In addition to email and cloud file sharing, messaging apps are among the riskiest channels for data loss, theft, or misuse in companies.[5] Smartphones are considered to be one of the most attractive gateways for cyberattacks. Viewed in this light, mobile security, in particular in terms of communication channels, must be prioritized accordingly. This is where our study uncovers deficits and contradictions:

- Among the companies surveyed, cybersecurity and data protection are top priorities when it comes to designing cybersecurity strategies; however, there is a surprising lack of urgency in terms of mobile security and the security of communication channels given today's increasingly mobile world of work. (Section 1)
- The majority of companies surveyed assume that private messengers are being used to communicate sensitive data and data worth protecting, despite being fully aware that these messengers are often insecure and do not comply with data protection standards. This fact strongly contradicts the assertion made by the majority of respondents that data privacy plays a vital role both in general and when it comes to choosing communication channels. (Section 2)
- Management and IT managers are aware of the potential personal liability associated with negligent and inadequate implementation of measures for ensuring cybersecurity and data protection. They are also aware that private chat apps do not safeguard user privacy or comply with data protection requirements. (Section 5)
- Nevertheless, the use of private chat apps is tolerated: the majority of companies surveyed tolerate the use of private messengers for business communication, while nearly one-fifth of respondents have no regulations in place regarding their usage in the business context. (Section 3)

[5] The Ponemon Institute: https://tessian.com/resources/ponemon-report-data-loss-prevention-on-email-2022/

Cyber Resilience and Maintaining Communication

For companies, reinforcing information security against cyberattacks has become a race against time. First and foremost, the goal is to prevent cyberattacks, which is a challenge, especially in view of the increasing complexity and frequency of attacks. At the same time, cyber resilience is required: companies need to be able to evade attacks without shutting down entire divisions. It is important to have the expertise needed to defend your company during a cyberattack while at the same time maintaining operational functionality. This includes a secure communication channel that is uncoupled from the existing IT infrastructure (keyword: out of band). Around one-fifth (22%) of all companies surveyed do not have an out-of-band communication tool in place for emergencies, with operators of critical infrastructures in a slightly better position (18%). (Section 6)

The Human Risk Factor: Protection Through Training

Planning a comprehensive cybersecurity strategy takes time and significant resources. All aspects must be considered, including the role of the individual as an interface and potential risk factor. Employees who are unaware of the potential risks lurking on the internet, how to safeguard themselves, and what they are and are not permitted to do pose a serious security risk. One wrong click is all it takes to introduce malware into a company, and improper actions can result in data breaches for which IT managers and management can be held personally liable. (Section 5)

Company secrets can easily end up in the wrong hands due to inadequately secured communication and collaboration tools, and corporate espionage and social engineering are topics that employees need to be made aware of. If employees are not properly informed about cyberthreats, it can lead to significant operational and financial damage, and also put the company's reputation at risk. The study shows that there is opportunity for improvement here (Section 1): only 16% of the companies surveyed prioritize end-user training as part of their cybersecurity strategy. Given the fact that humans are one of the greatest risk factors in terms of cyberattacks, it is important to raise awareness among employees through training and education.

Consistently Implementing Measures Across All Levels

Having a cybersecurity strategy in place is no longer optional for companies given the fact that they are facing a growing number of cyberattacks, let alone their obligation to comply with GDPR, NIS2, and other legal requirements. Nevertheless, according to our survey, more than one-quarter of the companies we surveyed are not yet prepared for the NIS2 directive to enter into force in October 2024 (Section 4). Now is the time for these companies to take their existing security awareness and apply it to all divisions, to implement measures consistently, and therefore to arm themselves against this constantly growing threat before it's too late. At the end of the day, the security of corporate communication channels is just as important as data protection and network security.

Threema.

Seriously Secure Messaging

Threema GmbH was founded in 2014. It's a pioneer of secure instant messaging solutions for individuals and organizations. The Swiss company operates its own servers in Switzerland and is known for its unparalleled metadata restraint and privacy protection. The Threema app is open source and counts more than 12 million users in Europe and beyond.

The business solution Threema Work has become a market leader in the German-speaking area and is used by over 8,000 companies, government agencies, schools, and organizations. Well-known corporations such as Mercedes-Benz Group, Allianz, Edeka, and TK Elevator use Threema Work as internal business messenger. Many small and medium-sized companies as well as public institutions (e.g., ADAC, Switzerland's federal administration, and the city of Frankfurt am Main) also use the service. Threema Work is particularly useful for fast, efficient, and secure communication in organizations, as a supplement to collaboration solutions, to contact non-desktop workers, and for confidential communication within the top management.