KONICA MINOLTA

# 360-DEGREE SECURITY

## FOR YOUR BUSINESS

Comprehensive **protection** for your IT, data, multifunctional and video security systems

WHITEPAPER SECURITY

Giving Shape to Ideas



# CONTENTS

# EQUIPPED FOR DIGITALISATION WITH COMPREHENSIVE PROTECTION

**In the age of digitalisation, companies must ensure their information security more than ever. According to a study by the Federal Office for Information Security[1], around 70 percent of German companies have been victims of cyber-attacks in the past two years.**

For example, WannaCry 2017, a ransom product, infected Deutsche Bahn video surveillance at railway stations and paralysed a Renault plant. At the end of 2018, it was the Trojan Emotet that caused enormous damage worldwide. Media companies, the chemical industry and energy companies are also being targeted, as evidenced by warnings from federal authorities. Attacks are often aimed at employees who open attachments, process files or do not properly back up computers as a vulnerability.

This shows that every company should consider whether it is prepared. After all, systems are becoming increasingly complex and require comprehensive protection, otherwise vulnerabilities and thus targets for cybercriminals open up. With increasing digitalisation, security is also becoming an increasingly important issue for medium-sized businesses.

It's not about whether a company gets targeted by an attack anymore. It's more about when.

To be properly prepared, companies need to know where potential vulnerabilities might be. Only those who know potential dangers can protect themselves against them. Only a comprehensive security concept creates real protection and allows companies to fully benefit from the opportunities offered by digitalisation. Thanks to its comprehensive portfolio and many years of expertise, Konica Minolta is in a position to professionally evaluate the security-relevant areas in companies and offer the right security solutions and services for all facets.

[1] The situation of IT security in Germany 2017, Federal Office for Information Security, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4



# SECURITY REQUIRES AN ALL-ROUND VIEW

**In order to obtain an overview of potential security gaps and the areas that need to be secured, it does not suffice to focus solely on the network and IT security.**

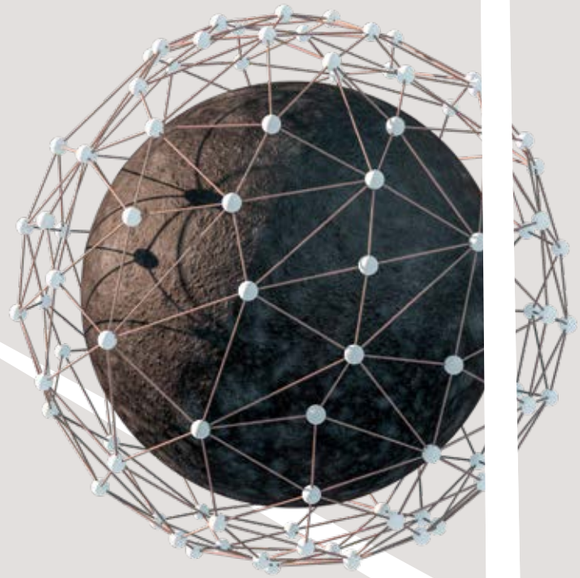
The multifunctional system (MFP) in the corridor, the field service tablet and the IP security camera are all part of the system landscape as networked devices. They all have attack surfaces.

However, companies often underestimate the need to implement a holistic strategic approach to security. Without this, there is no basis for security. Enterprises then either have no security solutions or solutions that are unsuitable for them. Another phenomenon in practice is that, although they are technically correctly equipped, they do not use the security solutions properly due to a lack of specialist knowledge.

The sources of danger that Konica Minolta's experts repeatedly encounter in their analyses are the lack of network access controls or inadequate password policies. If systems lack password protection or are easily overcome, they are easy prey.

This also applies to systems where not everyone thinks that they are part of the network as digital systems, so that intrusion can be possible via them. And that they have hard disks whose data must be protected. From webcams to video systems – in recent years there have been numerous cases where supposed standard devices have been infected by cyber attackers and used for attacks. In 2016, for example, almost 150,000 security cameras were hacked and misused as part of the well-known Mirai botnet for cyber attacks[2].

A company's own employees also play an important role in corporate security. Only with proper training can employees be sensitised to be less susceptible to social engineering – or to attacks that rely on employees clicking on e-mail attachments.



[2] New Jersey Cybersecurity and Communications Integration Cell, Mirai Botnet, 2016, https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet

# KONICA MINOLTA'S 360-DEGREE STRATEGY

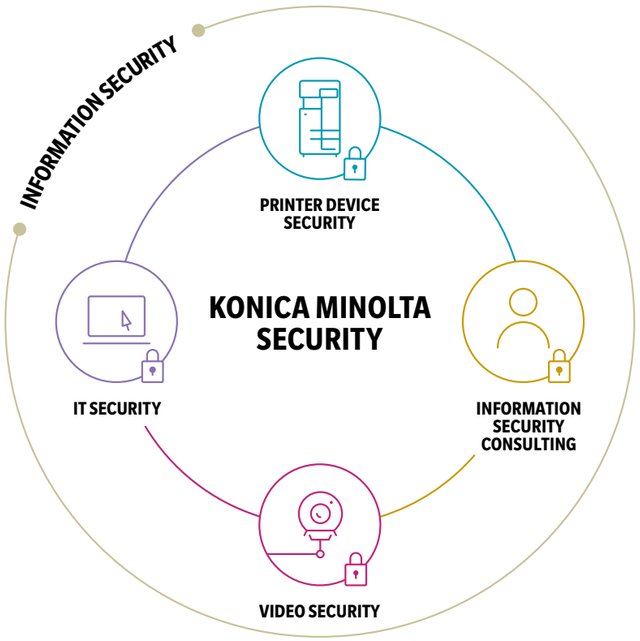
**Comprehensive security can only be achieved through a comprehensive information security concept. Therefore, Konica Minolta has adopted a 360-degree strategy that considers and covers all areas of a customer that are worth protecting.**

The experts first analyse the current security status using an ACTUAL analysis. Basic security (e.g. through firewalls and antivirus solutions), network access, mobile systems, encryption concepts, the access and data security of MFPs, the protection of building access and security-relevant areas, organisational principles and the level of awareness of employees are examined. This also includes penetration tests in which an attack is simulated because this is the best way to subject IT security precautions to a practical test and identify weak points. Nevertheless, according to a survey by the Bitkom industry association[3], only 17 percent of German companies use this option. Even audits by external specialists are only carried out by every fourth company.

Konica Minolta's 360-degree approach includes information security as well as technical and organisational solutions for IT security, multifunctional systems and video security in the area of terrain, building and process security, including the creation of awareness and training. Of course, the company also pays great attention to data protection issues.

Konica Minolta's concept development is based on the premise that comprehensive information security is only possible if areas such as IT security, data security, the protection of multifunctional systems and the security of any video security systems as well as building and perimeter protection are considered together.

Based on current analysis of the situation, the experts create a concept that is designed for the complete information security of the respective customer and his individual security requirements.




[3] Are German companies prepared for cyber attacks, Handelsblatt, 2018, http://veranstaltungen.handelsblatt.com/cybersecurity/cyberangriffe-deutsche-unternehmen-2018/



# MULTIFUNCTIONAL SYSTEMS

**Modern multifunctional systems (MFPs) are not just printers or copiers. MFPs are central document processing nodes in a company's network. It is therefore important to have appropriate access controls/rights to protect sensitive information in the form of printed documents or data stored in the system from theft.**

Because MFPs are not only part of the network, their own hard drives and main storage also contain potentially confidential and personal data. If companies do not have a security strategy and protection for their MFPs, this data can become easy prey for cybercriminals. In the worst case, it is not password-protected and confidential information temporarily cached on the system is not encrypted. Without deletion rules, sensitive data can also accumulate on the hard disk over a longer period of time. Even documents that are not to be printed represent a security risk that should not be neglected.

The Bitkom survey[4] "Economic protection in the digital world" from 2017 shows that 17 percent of the companies surveyed had physical documents, components or machines stolen. Another 14 percent of the companies suspect that they were affected, but do not know for sure. 30 percent of respondents said that IT and telecommunications equipment was stolen.

For a holistic security concept for MFPs, Konica Minolta offers a wide range of security functions within the bizhub SECURE framework. They cover three areas: access control/ access security, hard disk data security and network security. The first and most important step is to prevent unauthorised access to the system. This is done by using passwords or reading employee ID cards.

A critical point: security measures should always provide protection without compromising usability. This is not just to avoid creating new obstacles for users to slow down their productivity. When security measures are perceived to hinder them, users are less willing to comply. Passwords and user accounts not only allow companies to assign different rights to users, they also secure the system against unauthorised access. Functions that start document printing only after authentication also ensure that only authorised users receive documents.

## Check list

- Access control: use passwords
- Encrypt the hard disk
- Delete temporary data regularly
- Set up user accounts with individual rights
- Secure the hard disk against unauthorised access even if it is removed
- Control network security standards

[4] Economic protection in the digital world, Bitkom, 2017, https://www.bitkom.org/Presse/Anhaenge-an-Pls/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

# IT SECURITY

**Comprehensive information security also includes sophisticated IT security to protect digital information systems. Of course, network security is also part of IT security. For complete protection, however, much more must be considered – from organisational and technical basics to the integration of IoT devices or mobile devices and the human factor.**

A lack of knowledge or wrong behaviour of employees is often one of the biggest weak points. This is where companies should start – but according to Bitkom data[5], 47 percent of German companies do not train their employees in security measures.

Risk awareness at the decision-maker level is another necessary prerequisite. Companies have to be aware that they offer targets, therefore a protection concept is necessary. It should also be clear that security breaches will always occur. It is important to be prepared for this. Risk analyses and contingency plans increase risk awareness and reduce the dangers of possible damage. According to a Deloitte study[6], 58 percent of companies have a corresponding emergency plan.

Konica Minolta has developed a special analysis concept based on almost 20 years of experience. This concept forms the basis of its IT security analyses. In direct dialogue with the customer, what is considered during the analysis is individually defined because nobody knows the data and requirements as well as the company itself. To start with, the experts carry out detailed actual/target analyses to identify not only the given conditions, but also the individually necessary security measures.

Thanks to the 360-degree view of the company's own processes and the systems and solutions used, transparency is created. This shortens response times and increases the level of security.

### Check list

- **Perform risk and protection needs analysis**
- **Create or revise a security strategy**
- **Implement information security processes**
- **Establish or expand technological measures such as authorisation management, encryption or mobile device control**
- **Sensitise employees – conduct an awareness campaign**
- **Verify technical solutions through penetration tests**

[5] Economic protection in the digital world, Bitkom, 2017, https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

[6] Cyber-Security Report 2017 – Part 2, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf



# VIDEO SECURITY

**Of course, modern perimeter and building protection also includes IP video systems. According to the Bundesdruckerei study[7] "Digitalisation and IT security in German companies," this is still lagging behind the virtual protection measures.**

On the other hand, they can support smooth production processes by detecting irregularities in processes or overheating of machines and then triggering a message or automatically stopping processes. But there are several aspects to consider when setting them up. One is that networked video cameras, as part of the corporate network, are also networked devices, so they must be subject to the same security measures as all other IoT devices. The same applies to any storage devices or hard drives, especially when people are being recorded.

When setting up a video security system, you should first clarify what images are required because high-resolution recordings entail a much larger amount of data, for which the network may not be designed. This determines whether the cameras should be integrated into the existing productive network or whether a separate parallel network should be set up.

In addition, the same aspects apply as for networked devices: The systems purchased should in any case have configuration and backup tools in order to harden them when used appropriately and thus protect them from unauthorised access. And data transmission should be encrypted. Otherwise, unauthorised persons may be able to access this data under certain circumstances or penetrate the corporate network via poorly secured IP cameras.

When setting up video security, data protection aspects must also be taken into account: which areas should be secured? How long does data need to be stored and who has access to it? Konica Minolta recommends an approach to selection and implementation that includes consulting workshops to determine requirements, update the works council and data protection officer on the state of the art at an early point in time, and describe operational requirements, purpose, and justification together.

### Check list

- **Define demand: What camera power is required?**
- **Check network capacity**
- **Define operational requirements, purpose and justification**
- **Secure data and data transmission using encryption**
- **Ensure that the recording is handled in a manner that conforms to data protection requirements**

[7] Study: IT Security as part of Digitalisation, Bundesdruckerei, 2018, https://www.bundesdruckerei.de/de/studie-it-sicherheit

# INFORMATION SECURITY CONSULTING

**The protection of the information in the company – whether it is the company's own information or that of customers – is one of the main goals of information security concepts because this information is the crown jewel that attackers are targeting. According to the Bitkom survey[8] "Economic protection in the digital world", 23 percent of German companies have been victims of data theft in the last two years. Another 18 percent suspect that they were affected.**

The targets range from communication data (48 percent), customer data (20 percent) and financial data (20 percent) to intellectual property or employee data.

Information security and data protection are central values that are extremely relevant for business success, competitiveness and reputation. In addition, legal regulations such as the EU Basic Data Protection Regulation (GDPR) also require them – including concrete protective measures to be taken. According to the Bundesdruckerei study[9] "Digitalisation and IT Security in German Companies", 75 percent of companies have at least rules for handling sensitive information, 81 percent have defined access rights for sensitive information. The rest is in arrears.

Here, too, companies must see to it that their employees are made aware of the issue – awareness of the dangers and consequences in the event of a security breach is not always clear. Companies should first determine what protection they need. Konica Minolta defines this need through appropriate analyses. The target state derived from this is achieved not only through the use of technical solutions, but also through targeted employee training and workshops on the sensitivity and relevance of information security.

Information security includes, for example, solutions for access security: the more sensitive data is, the more important it is to restrict the group of people who have access to it. Passwords alone are not enough. Valuable information should also be encrypted under certain circumstances. Not just since the GDPR came into force is it also advisable to have an overview of which personal data a company has collected. It is also important to ensure that there is only one central, up-to-date data record and not different versions distributed across the network.

Information security also includes protected transport – information must be securely transmitted end-to-end in encrypted form.

In the event of violations, it is also crucial to have protocol data at hand so that it can be made available. Not only does it allow infringements to be identified quickly, log data is also required for damage assessment and mitigation.

[8] Economic protection in industry, Bitkom, 2018, https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf

[9] Study: IT Security as part of Digitalisation, Bundesdruckerei, 2018, https://www.bundesdruckerei.de/de/studie-it-sicherheit



## Check list

- **Carry out risk and protection needs analysis and define information worth protecting**
- **Define an information security concept with guidelines**
- **Implement information security processes**
- **Establish or expand technological measures such as authorisation management, terminal device security solutions, encryption or mobile device control**
- **Use solutions that provide an overview of personal data and comply with the reporting obligations of the GDPR**
- **Sensitise employees to the safe handling of information – conduct an awareness campaign**
- **Verify technical solutions by conducting penetration tests**

KONICA MINOLTA

# STRONG PARTNER AT YOUR SIDE

**Modern IT offers great potential for companies. In order to be able to tap this potential safely, they need a well thought-out, comprehensive security strategy. A partner like Konica Minolta is at your side as a consultant.**

Small and medium-sized enterprises in particular do not usually have the resources to keep a constant eye on the complexity of their infrastructure and potential weaknesses. A strong partner can help them to define and implement an individual security concept for comprehensive protection with sound advice and well thought-out solutions. Konica Minolta can also take care of its operation and maintenance as well as regular training of employees.

Konica Minolta's 360-degree approach increases effective security for corporate information, IT, multifunctional systems, buildings, and manufacturing. Companies also benefit from resource and cost savings as Konica Minolta provides them with a customised solution that meets their security needs and avoids additional effort and costs.

If desired, companies can also have Konica Minolta employees fulfil the role of their Chief Information Security Officer (CISO). Such outsourcing is particularly interesting for small and medium-sized enterprises that do not want to build up excessive resources of their own for their information security.

## WOULD YOU LIKE TO LEARN MORE ABOUT OUR SECURITY OFFERS OR HAVE A FIRST MEETING WITH US?

**konicaminolta.eu/security**

Konica Minolta
Business Solutions Europe GmbH, Europaallee 17, 30855, Langenhagen · Germany
Tel.: +49 (0) 511 74 04-0, Fax: +49 (0) 511 74 10 50, www.konicaminolta.eu 