KONICA MINOLTA

INTELLIGENT SECURITY

SOLUTIONS FOR YOUR BUSINESS

Whitepaper Security

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

Giving Shape to Ideas

CONTENTS

IN THE AGE OF DIGITALIZATION, COMPANIES MUST ENSURE THEIR INFORMATION SECURITY MORE THAN EVER.

Many organizations do not have the resources to keep a constant eye on the complexity of their infrastructure or potential weaknesses or threats but they need to consider whether they are prepared and if they have the know-how and resources to perpetually monitor their situation.

Systems are becoming increasingly complex and require comprehensive protection, otherwise vulnerabilities exist and they become targets for potential security attacks. With increasing digitalization, security is also becoming an increasingly important issue for medium-sized businesses. It is not about whether a company gets targeted by an attack anymore. It's more about when.

A comprehensive security concept creates real protection and allows companies to fully benefit from the opportunities offered by digitalization.

Thanks to an extensive 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 IT security, data security, multifunctional system security and intelligent video solutions security.

SECURITY REQUIRES AN INCLUSIVE 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.

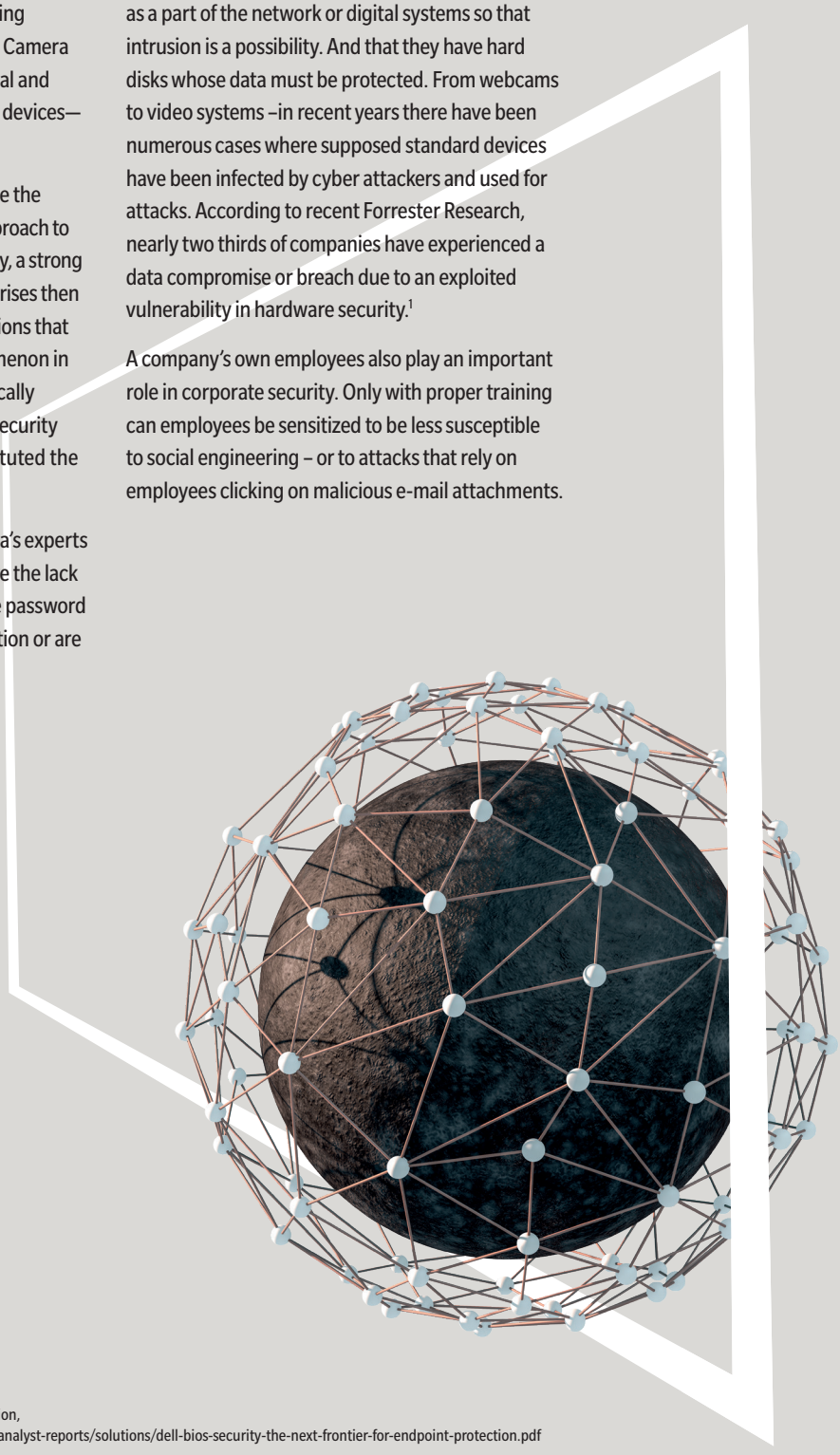
The multifunctional peripheral in the corridor, the field service tablet accessed performing routine maintenance and the IP Security Camera monitoring activity— all part of the normal and customary system landscape as network devices— and they all have potential attack points.

However, companies often underestimate the need to implement a holistic strategic approach to security. Without this type of methodology, a strong security foundation does not exist. 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 and/or have not instituted the required security policies.

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 that individuals neglect as a part of the network or digital systems so that intrusion is a possibility. 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. According to recent Forrester Research, nearly two thirds of companies have experienced a data compromise or breach due to an exploited vulnerability in hardware security.[1]

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



[1] BIOS Security – The Next Frontier for Endpoint Protection, https://www.dellemc.com/en-us/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf

KONICA MINOLTA'S 360-DEGREE STRATEGY

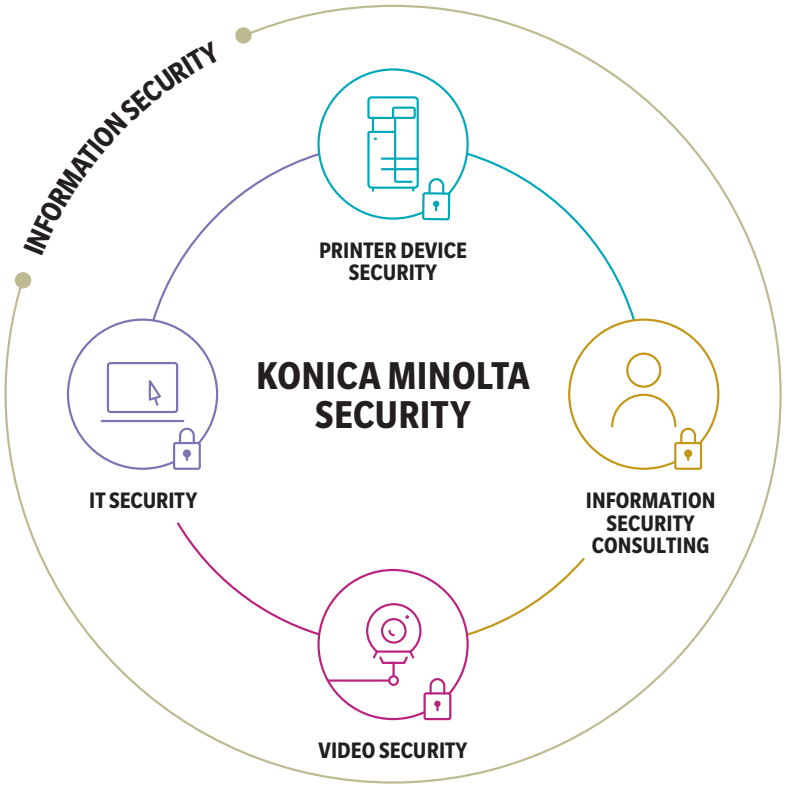
Comprehensive security can only be achieved through a comprehensive information security concept. Therefore, Konica Minolta has adopted a 360-degree strategy that considers and covers all areas of a customer's environment that require protecting

The experts first analyze the customer's current security status. 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, organizational 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.

Konica Minolta's 360-degree approach includes information security as well as technical and organizational solutions for IT security, multifunctional systems and Intelligent Video Solutions security in the area of terrain, building and process security, including the creation of awareness and training.

Of course, we 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 the protection of buildings, perimeters and people are considered together.



MULTIFUNCTION PERIPHERAL PRINTERS

Modern multifunctional printer 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, scanned 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. Data can become easy prey for cybercriminals. In a worst case scenario, if this data is not password-protected and confidential information is temporarily cached on the system and is not encrypted, the customer has a serious vulnerability.

Without deletion rules, sensitive data can also accumulate on the hard disk over a longer period of time.

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 unauthorized 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 authorized users receive documents.

It is also essential for businesses to be aware of unauthorized MFP use by authorized users. This is a key source of data breaches for organizations because many companies do not know who used the MFP, what they used it for or when they used it. This potentially leaves them liable since data breaches at the MFP may expose an organization's important trade secrets, intellectual property information, as well as customer, patient and employee data and personally identifiable information (PII).

Through technology available through Konica Minolta, organizations gain access to information on who used the MFP, for what and when, and supplies a user-configurable breach alert system to help maintain data integrity.

Additionally, The LK-116 BitDefender® Virus Scan Functions provide added security for documents processed at the MFP, inclusive of print data, scan transmission data, Internet Fax transmissions and receptions as well as data that is saved or retrieved from the Solid State Drive (User Box, SMB folders, etc.). Applications, Multimedia data, certificates, etc. saved on the MFP are also protected. The embedded Konica Minolta malware detection system constantly monitors the data exchanged between the MFP and the external environment.

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 unauthorized access even if it is removed
- Control network security standards

IT SECURITY

A Comprehensive Information security strategy begins with evaluating risks. The strategy requires a lifestyle approach that takes into consideration evolving threats and a multi-layer solution. Efficiently and effectively deploying and managing security solutions lowers risk levels.

Risk awareness at the decision-maker level is another necessary layer. Companies have to be aware they offer targets; therefore a protection concept is necessary. It should be clear 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 study3, 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 which takes into consideration every individual business and their needs. Experts determine a detailed plan and specific security measures.

Thanks to the 360-degree view of the company's own processes, 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 vulnerability management, security monitoring (SIEM), encryption or mobile device control
- ☑ Sensitize employees – conduct security awareness training and testing
- ☑ Verify technical solutions through penetration tests

[3] 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 IP SURVEILLANCE SYSTEMS

Intelligent Video Solutions combine visual intelligence, thermal, sound and sensor data to better protect people, facilities, and infrastructure. With secure video security & surveillance, situation analysis and access control.

IP Video systems can support production processes by detecting irregularities in processes or overheating of machines and then triggering a message or automatically stop a process.

Combined with thermal imaging, this technology ensures reliable detection of moving objects, even under the most challenging light conditions and over long distances. Thermal imaging is an indispensable part of many security and surveillance applications. An increasing number of industrial companies, public institutions, authorities and agencies use thermal imaging technology to protect their assets and personnel,resulting in a greater return of investment.

In contrast to cameras with optical image sensors, a thermal camera can detect extremely small temperature differences and visually display them using colors for quick and easy identification of the situation. Intelligent video solutions are optimized for remote applications and cloud-based technology. In simple terms these solutions are computers with lenses, working intelligently and with embedded storage capacities.

There are several aspects to consider when setting up an IP video system. 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.

VIDEO SECURITY

The protection of information – 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.

When setting up a video security system, you should first clarify what it is you want to see and exactly what images are required. Network utilisation should also be considered, High-resolution recordings entail a much larger amount of data, for which the network may not have been previously designed. Calculations should be made to decide whether the cameras should be integrated into the existing productive network or whether a separate parallel network should be installed.

In addition, the same aspects apply as for networked devices: The systems purchased should in any case have configuration and backup tools to ensure system integrity and protect them from unauthorized access. Any data transmission should be encrypted, otherwise unauthorized persons may be able to access this data or penetrate the corporate network via poorly secured IP cameras.

When setting up video security, data protection aspects must also be taken into account, looking at which areas should be secured? How long data needs to be stored for and who has access to it? Konica Minolta recommends an approach to selection and implementation that includes consulting workshops to determine requirements, to help understand the 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

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.

Information security and data protection are central values that are extremely relevant for business success, competitiveness and reputation. In addition, legal regulations such as HIPAA, PCI, CCPA, CMMC and other regulations require them – including concrete protective measures to be taken.

Together with All Covered, 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. It is also important to ensure 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 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

Check list

- ☑ **Carry out annual risk assessment for continuous compliance with regulatory requirements like HIPAA, CCPA, PCI etc.**
- ☑ **Define an information security concept with guidelines**
- ☑ **Implement information security processes**
- ☑ **Establish or expand technological measures such as vulnerability management,security monitoring (SIEM), authorization 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 industry, state and federal required regulations**
- ☑ **Sensitize employees to the safe handling of information – conduct security awareness training and testing**
- ☑ **Verify technical solutions by conducting penetration tests**

A 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.

Many organizations do not have the resources to keep a constant eye on the complexity of their infrastructure, potential weaknesses and threats.

Konica Minolta can help to define and implement an individual security concept for comprehensive protection with sound advice and well thought-out solutions. We can also take care of its security operation and maintenance as well as training employees.

Konica Minolta's 360-degree approach increases effective security for corporate information, IT, data, multifunctional systems and video security systems, but most importantly it protects people, facilities and infrastructure.

LET'S TALK

WOULD YOU LIKE TO LEARN MORE ABOUT OUR SECURITY SOLUTIONS OR ARRANGE A MEETING WITH US? PLEASE VISIT:

HTTPS://KMBS.KONICAMINOLTA.US/KMBS/IT-SERVICES/IT-SECURITY/MANAGED-SECURITY-SERVICES

For complete information on Konica Minolta products and solutions, please visit: CountOnKonicaMinolta.com

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446
CountOnKonicaMinolta.com

Item #: IVSSECURITYWP
12/2020-Z