thínkproject

The building blocks of information security

Constructing secure foundations for you and your providers

Contents

03 **Billions invested in information security and data protection across Europe**

13 **Breaking down the terminology**

- Understanding information security
- Clarity on data protection

16 **You've got the digital strategy, now what about the information security?**

- Digital change is good, but be mindful of your vulnerabilities
- How you and your stakeholders can protect valuable data

17 **Developing your own information security strategy**

20 **Insights from the Expert**

23 **Information security trends every business should know in 2024 and beyond**

24 **Be proactive to overcome security threats**

Billions invested in information security and data protection across Europe

Data protection and information security isn't just a hot topic, it is a crucial strategy for businesses to protect their most valuable information assets.

Kroll's 2021[1] report into data breach trends identified the construction sector as seeing an

800%

increase in reported data breaches between 2019 and 2021, compared with an

133%

average increase, across other industries.

Contributing factors include difficulties in managing data collaboration between firms, control of assets in a geographically dispersed environment (including remote working) and an increasing exposure to IoT based threats as the sector innovates. These challenges have highlighted to IT and compliance leaders the importance of ensuring their digitisation and security strategies are effectively meeting these challenges.

1 www.kroll.com

Investment in information security shows no sign of slowing

According to the IDC (International Data Corporation), IT security spending in Europe was predicted to reach approx.

€47 billion
in 2022

with a five-year forecast assuming investment will surpass

€66 billion
by 2026[2].

Information and cyber risk management is branching out from the sectors that have been strong investors. The digitisation of construction processes and the move towards DfMA (Design for Manufacturing and Assembly) that shifts the construction industry into the manufacturing sector, brings with it these investment pressures.

2 www.idc.com

Data protection is now a necessity for every business

Alongside and closely linked to the above is the protection of personal data. Any business within the EU is now well aware of the General Data Protection Regulation (GDPR), which has introduced strict regulations around data privacy, both from the point of view of the customer, and of the business. Data protection serves to both protect your own company (personal) data, and ensure you are protecting the (personal) data of your customers, supply chain and stakeholders.

Alongside this, the Network and Information Systems Directive (NIS Directive) defines measures to ensure a high common level of security of network and information systems in the EU. The NIS directive created a uniform legal framework for the EU-wide development of national cyber security capacities, greater cooperation between the member states of the EU, and minimum security requirements and reporting obligations for critical infrastructures, as well as for certain providers of digital services such as cloud services and online marketplaces.

Whether GDPR or NIS – both significantly contributed to increasing awareness and conversation around both data protection and information security in every business.

Types of security breaches that users are most susceptible to

Giving employees regular information security training reduces the risk of a successful attack.

Malware

This malicious software is designed to harm your computer system and network. Malware can come in many shapes and forms, from viruses to spyware and more.

Businesses can be vulnerable to this type of attack as malware can be disguised as links in emails for example, making it easy to fool users who are not vigilant.

Ransomware

Ransomware can be particularly devastating as it can lock your important files and demand payment to regain access.

Every business has valuable data that cybercriminals want to gain access to, and ransomware can spread rapidly through a network, affecting all aspects of the business.

Phishing

Phishing criminals will impersonate trusted colleagues to attempt to gain access to your network. This is usually through password resets or clicking on links.

Once access has been given, ransomware or other harmful software can be installed on the system, or data can be stolen.

Advanced Persistent Threat

An Advanced Persistent Threat (APT) is when a well-trained, typically state-controlled, attacker attacks a network or system in a very targeted manner for the purpose of espionage or sabotage over an extended period of time, possibly moving and/or spreading within it to gather information or manipulate.

Social Engineering

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons.

There are many well documented attack techniques which are often used in combination to compromise a business:

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Large quantities of data bombard a website or application with the intent using up all of the available network bandwidth or processing power of the system, rendering it unavailable. While they are disruptive, by themselves DDoS attacks are normally short lived and rarely do permanent damage, however they are often used as a diversionary tactic to take focus away from a more serious attack taking place at the same time.

Man-in-the-Middle Attack (MitM)

Man in the Middle attacks can be tricky to achieve, however, if successful they can allow an attacker to see data in plan text (e.g. passwords, project data and emails) which is normally encrypted. Threat actors may also be able to manipulate data as it is sent.

Insider Threats

An insider threat is someone that has a level of authorisation within an organisation and acts in a way which breaches security. This may be malicious or unintentional, however the risk to a business is elevated because of the level of access to data and systems they already have.

SQL Injection

Attackers use SQL injection vulnerabilities to manipulate, delete or extract data from an application without proper authorisation. This can lead to large scale data thefts and system corruption.

Cross-Site Scripting (XSS)

Harmful scripts can be amended into websites, which then spy on a user's activity through their browser without their knowledge. Attackers attempt to have their target run their malicious code by serving it from a trusted website. There are many vulnerabilities that allow XSS attacks and they can be difficult to stop because the victim's web browser believes the script is coming from a trusted website.

Password Attacks

This attack can be implemented in several ways, such as password cracking, to gain access to passwords, which can then be changed or decrypted. Weak passwords can be guessed with enough time, however criminals exploit our tendency to use the same password in many locations by trying username and passwords from public data breaches to sign into other websites and systems. This has been a very successful technique in recent years.

Zero-day Exploits

When an attacker exploits an unknown vulnerability, the ability for security teams to detect and respond to the threat is greatly reduced. When discovered, it will normally take a few days for software vendors to create a patch for the exploit. This exploit is known as a 'zero-day' because is has been known about for zero days.

Malware

Spyware | Worms
Trojans | Viruses
Ransomware

Network-based

Dos | DDos
MitM

Web-Application

XXS
SQL Injection

Social Engineering

Phishing
Insider threats

Zero-day Exploits

Attacks on undisclosed vulnerabilities

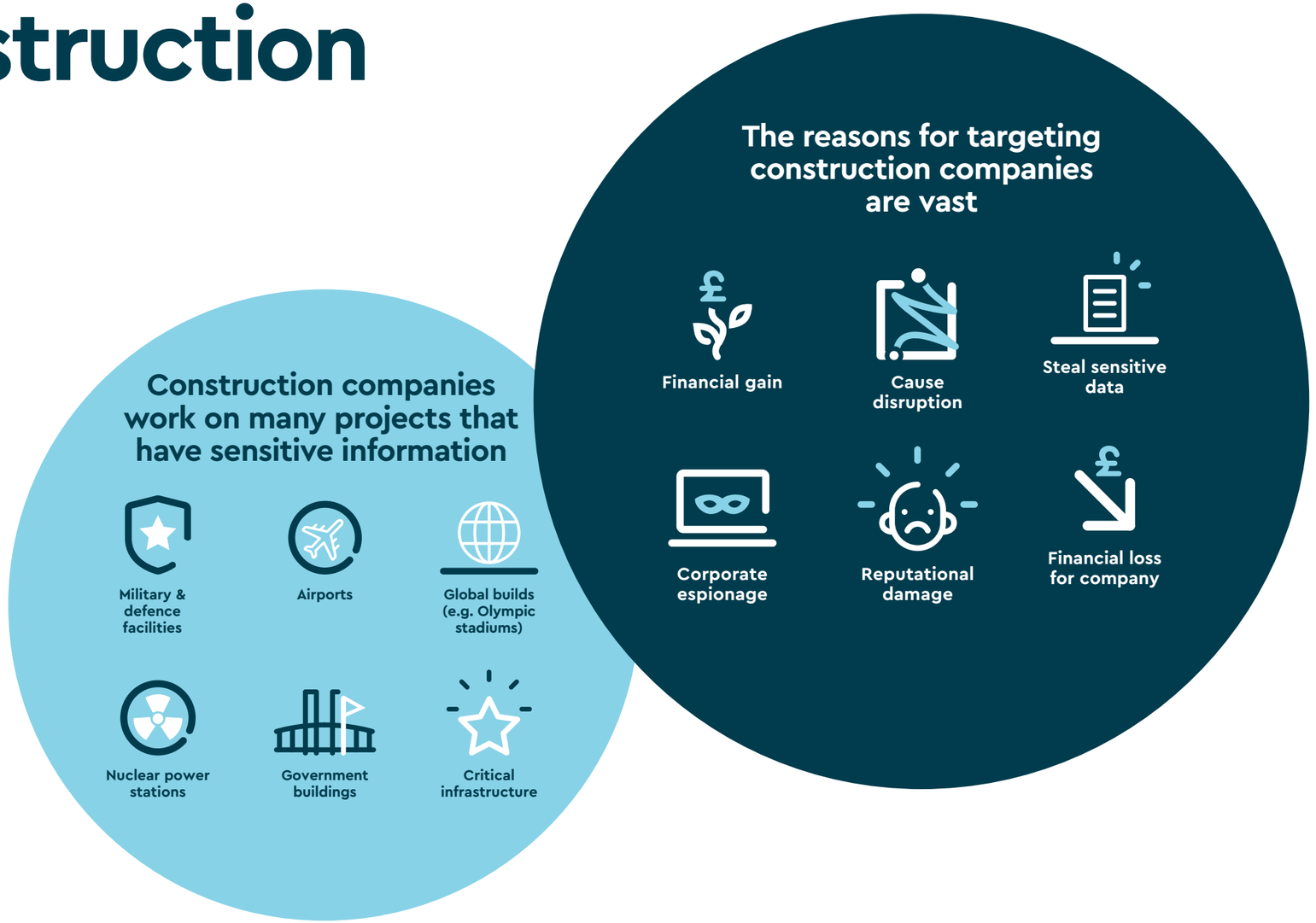
Authentication

Password attacks

The construction sector is not immune to information security breaches

Many strides have been made towards digitising the construction industry. The use of automation, AI and digital methods such as building information modelling (BIM) all require software which benefits construction by improving quality while saving on time and costs, as well as providing insights and analysis on past data. These are all positive steps in an industry that has typically been seen as lagging in digitalisation in the past. However, with an increased digital presence the risk of malicious intent is always quick to follow.

Why is construction targeted?



How a breach of information security can affect a business

Picture this scenario, cyber criminals sending a phishing email to one of the employees of a multi-national construction company who opens a link contained in this email, followed by ransomware that locks the contractor out of their project data while crippling several project sites.

Hackers not only gain access to personal data of employees and customers, as well as sensitive information on construction projects, such as blueprints for government buildings across the globe but this cyber attack also leads to massive ramifications for the business, its stakeholders, supply chain and its customers. Not being able to access project data and continue work as planned has a big impact on the overall schedule with potential penalties for late delivery and can lead to a big loss in productivity. Overall, the financial and reputational damage for the company can be significant, the monetary repercussions even more so. The company is now responsible for covering legal fees, remediation costs and substantial fines. Just as importantly, trust in the company has spiralled and considerable effort, resources and money will be needed to rebuild it. The risks of trying to recover from an attack can be even worse for industries with very sensitive data, such as the nuclear sector or for critical infrastructure, where potential problems could be felt country or worldwide.

The company tackled this by developing an information security strategy to ensure this wouldn't happen again, including multi-factor authentication, training for employees to recognise phishing scams, strengthening network security and improving their incident response procedures. On top of this, they also developed a policy of rigorous vetting for any external providers they were working with to make sure the entire chain had similar procedures in place. These steps ensure that if another breach is successful, the organisation is prepared and thus the risk is minimised.

This example shows the risks that construction companies can be vulnerable to, and how prioritising information security is a benefit in the long run. The stakes become even higher when cybercriminals intend to disrupt sensitive projects, such as critical infrastructure[3] or nuclear facilities. In 2021, 56% of energy facilities in the US reported attempted cyberattacks that paused operations, with one attack estimated to cost $100 billion to recover from[4]. The reach of the effects of these infrastructure attacks can be far and wide, from water supplies to heating or lighting homes.

3 www.allianz.com

4 www.firstpoint-mg.com

This information security brochure aims to deliver insights that could help your company stay on top of best practices, tell you what you should look for in your external providers and how to stay safe.

Breaking down the terminology.

Understanding information security:

Information security can involve many acronyms and technical language.
Use our guide for the most popular terminology to stay in the know.

Access Control
The method of ensuring that individuals only have access to data for which they have a need and permission. These controls are essential for minimising the scope of a data breach.

BCP
The Business Continuity Plan is developed and enacted during an emergency and defines response actions and recovery steps to ensure that the business continues to function during the crisis.

BIA
A business impact analysis quantifies the potential impact of a threat to business operations. This is a key step in defining appropriate controls to reduce risks to an acceptable level.

CIA Triad
A common three-point model that includes Confidentiality, Integrity and Availability which are the three main principles of information security.

CISO
The Chief Information Security Officer is a professional responsible for overseeing and managing an organisation's information security program. The primary role is to protect the confidentiality, integrity, and availability of the organisation's information assets.

Firewall
A device which controls the flow of data between networks.

Incident Response
The process of managing the identification, containment and removal of a security threat and the recovery back to a normal state.

Information Security
Refers to the protection of information confidentiality, availability and integrity (see: CIA Triad), as well as the actions taken to prevent harm. It involves implementing measures and adopting best practices and can include computer networks, on-site buildings and anywhere else where information can be found.

ISMS
The Information Security Management System encompasses policies, processes and controls to protect and prevent an organisation's sensitive information from attacks.

ISO 27001
Globally recognised as the most accepted and implemented of ISMS. ISO have created a robust framework for companies to follow to ensure maximum protection and offer accreditations to organisations that meet the criteria.

Patching
The process of applying software or firmware updates to remove vulnerabilities from your assets.

Risk
When a vulnerability and a threat combine.

Risk Assessment
A mechanism put in place to rate risks and their severity.

Threat
Any action that could cause harm.

VPN
A Virtual Private Network secures communication between two networks or between a user's device and their corporate network, by sending it in an encrypted tunnel. A VPN has encryptions to keep identifiable information blocked to potential threats. These are typically used when accessing the internet.

Clarity on data protection

Effective data protection starts with an understanding of these common terms:

Data Breach
A security incident in which unauthorized parties gain access to sensitive data or confidential information, including personal data, or corporate data

Data Controllers
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Minimisation
The act of minimising the collection of personal data to that which is necessary for the performance of the processing activity.

Data Processing
Data processing refers to the collection, analysis, and transformation of data to extract meaningful information and facilitate decision-making. It plays a crucial role in numerous fields, including business, research, and technology, enabling organisations to leverage data for operational efficiency, strategic planning, and innovation.

Data Processors
Any entity which processes personal data on behalf of the controller.

Data Protection
Control over the access and use of data.

Data Protection Officer (DPO)
The Data Protection Officer is a role established by the GDPR. The primary role of the data protection officer (DPO) is to ensure that the organisation, for which the DPO has been appointed, processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Data Subject
Any person who can be identified as natural person by the data collected about them.

DPIA
The Data Protection Impact Assessment is a process used to identify risks and the impacts of processing and storing data on an individual. The DPIA is most commonly used when processing special category data or for large scale and high risk data processing activities.

DSGVO
DSGVO stands for 'Datenschutz-Grundverordnung', which is the German term for the General Data Protection Regulation (GDPR).

Encrypted Data
This is data that has been scrambled into secret code that can only be unlocked with a unique digital key. Encryption is used to prevent it from being read by unauthorised persons, or stolen, changed, or compromised. This is a particularly powerful control if data is lost or stolen.

GDPR
The General Data Protection Regulation is a privacy EU law that created a consolidated data protection legal framework across all European Union member states (EU) and Iceland, Liechtenstein, Norway, and Switzerland – which are part of the European Economic Area (EA) single. market. Coming into effect in May 2018, the GDPR applies to processing of personal data of EU citizens, irrespective of whether processing takes place in the EU or outside EU.

Personal Data
Any information that that relates to an identified or identifiable individual (names, email addresses, IDs, etc).

PII
Personal Identifying Information (PII) is any type of data that can be used to identify someone, from their phone number, passport information, and social security numbers.

Basic terms on data protection

SAR

A Subject Access Request is a mechanism that allows individuals to ask for a copy of their data, held by an organisation. They may also be used by individuals to enact their rights, such as the right to rectification or the right to be forgotten.

Seven Main Principles

The GDPR operates under seven main principles: Lawfulness, Fairness & Transparency, Purpose Limitation, Data Minimisation, Accuracy, Storage Limitations, Integrity & Confidentiality, and Accountability.

Special Category Data

A well defined subset of personal data which is considered sensitive, such as race, ethnicity, sexuality or political opinions, and whose processing is subject to additional requirements.

UK Data Protection Act (2018)

The UK's data protection law covers UK citizens and combines GDPR aligned controls with wider data protection topics.

You've got the digital strategy, now what about the information security?

Recent years have seen an acceleration of digital transformation and business process change across the Architecture, Engineering, Construction and Operations (AECO) sectors.

Recent years have seen an acceleration of digital transformation and business process change across the Architecture, Engineering, Construction and Operations (AECO) sectors.

The rise of digitalisation, Construction 4.0 and AI technology certainly ramped up during the 2020 pandemic, with companies increasingly seeing the benefits of construction intelligence translating into increased efficiency, productivity and better sustainability and health & safety.

Focusing on a digital strategy could involve many different pieces of software, such as BIM and CDE platforms, and builds a very useful toolkit across the entire construction project lifecycle. As well as saving on time and costs, what is becoming increasingly valuable is the data and analytics that can now be collected to give important insights that benefit future projects.

Digitalisation is great, but be mindful of your vulnerabilities

Digitalisation has vastly increased the amount of data that is collected, processed, and stored. This data often includes sensitive customer, financial, and personal data as well as IP and commercially sensitive information. The depth of data held has raised the profile of AECO organisations and their supply chain to the cyber-criminal community, increasing the risk of being targeted by a range of threat actors from ransomware groups to state sponsored Advanced Persistent Threats (APTs).

For a threat to be successful, it needs to exploit a weakness, whether a technical weakness, such as a software bug, a procedural weakness, or copying data to a USB drive without encrypting it, or a human weakness, such as being fooled by a scam email.

Protection from compromise traditionally requires an information security strategy which ensures that digital systems are maintained, renewed, monitored, secured, and resourced across their lifecycle, often to strict technical and compliance standards (ISO27001, SOC2, NIST-800, Cyber Essentials Plus, etc). Staff must be trained in processes and made aware of cyber threats and the threats themselves need to be identified and remediated quickly to ensure that attackers do not have time to damage the network. All of this not only requires a large commitment from the company in information security and data protection but also significant investments.

Adding to the challenge for the AECO sector is an increasing need to manage access to data in a cross organisation collaborative environment, bringing together users from different organisations, with different security standards and policies while ensuring that the client's requirements are met. The tools that you use need to provide flexibility and enforce security controls that do not rely upon any one organisation to maintain.

From what we can gather from examples of information security breaches, cyberattacks will lead to significant disruption, financial loss and damage to reputation. What is particularly important when it comes to security for construction companies is the valuable data that could fall into the wrong hands. Construction software handles a lot of sensitive information, from blueprints, designs and plans to data around weak spots in buildings or other faults that can be exploited. This sensitive information is required to build high-quality projects; however, it can also work against a company if hackers gain access.

Lastly but no less important is the commitment for companies to protect their employees, customers and the entire supply chain's data. A breach of personal data could result in lengthy legal proceedings and fines, not to mention substantial reputational damage that can take a long time to recover from.

How you and your stakeholders can protect valuable data

Digitalisation has increased interconnectivity and collaboration between different stakeholders involved in a construction project, including architects, engineers, contractors, and suppliers. This increased connectivity has numerous benefits, but also carries a risk that security breaches affecting one party can quickly spread throughout the project ecosystem, affecting others as well.

Construction companies need to prioritise information security by implementing robust security measures, such as patch management, security monitoring, access control, encryption, and network segmentation, to protect their systems and data from cyber threats. They also need to ensure that their employees are trained in security best practices and are aware of the risks of cyber-attacks. By taking proactive measures to protect their systems and data and having a knowledgeable workforce, the risk of attacks can be minimised and ensure the whole supply chain can thrive and build the best assets they can with digital technology.

Developing your own information security strategy

That all sounds good on paper, but what are the key points to cover when planning an information security strategy? You might consider the following:

- A defined goal to work towards, and the objectives for getting there. This could mean building trust with a customer base, having a plan in place for business continuity or certifying against a recognised information security standard.
- A thorough risk assessment that identifies points of weakness in the storage and processing of data. Ideally focusing on your areas of highest risk first.
- Establishment of an Information Security Management System (ISMS) team to own the governance and controls required for maintaining solid data protection standards.
- Development of incident response and business continuity plans, so that work can continue in the event of a security breach.
- Established roles and responsibilities will make information security run smoother. With clear decision makers and sufficient resource allocation, you should not be caught out in a worst-case scenario.
- Continuously review and develop policies and procedures, as well as organise regular reviews of incidents. The best outcomes for any process come from collaboration.
- Drive a culture in which everyone takes responsibility for the protection of data. Coupled with regular training and simulated attacks, organisations must ensure their teams are regularly refreshed on the dangers of threats such as phishing scams.
- Getting assessed by an external provider. This is much more than a tick box that gives you a badge for your website. These external assessments can identify gaps in security plans that may not be as apparent to someone using the network every day.

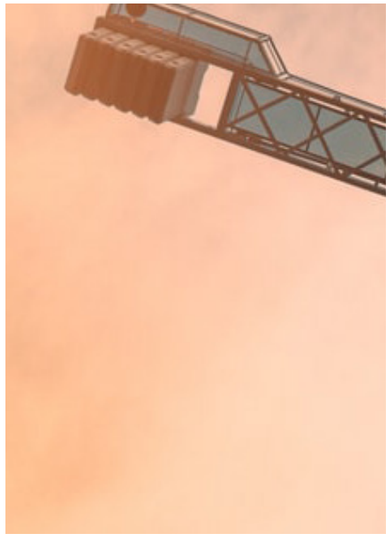
The gold standard in security to look for in your provider

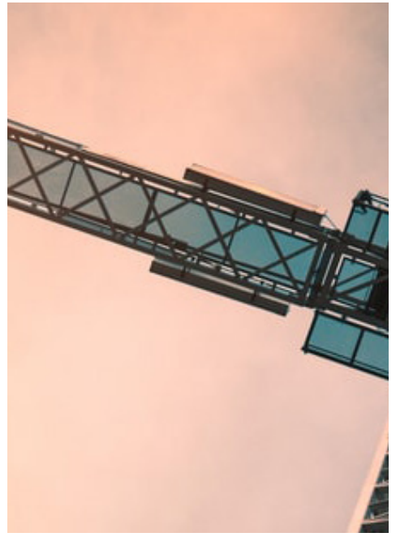
Let's take a deeper look at what you should expect from a software provider that cares about the security of your data.

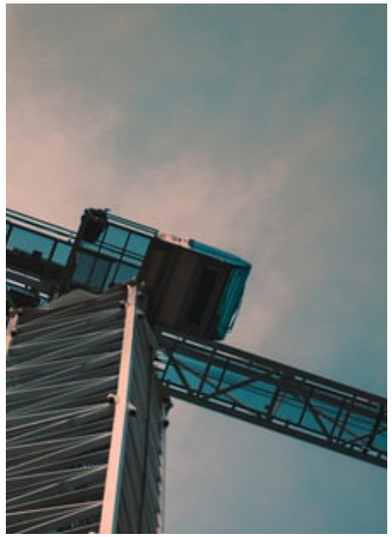
Security Type	What does this mean?	At Thinkproject
Secure Development Practices	Development teams should be using tools to structure their work and the delivery of new code into a released state. The delivery should include mechanisms to identify and fix component and code level vulnerabilities, should align to best coding practices and testing of code should be automated where possible	Thinkproject works within a defined DevOps structure using CI/CD (Continuous Integration/ Continuous Delivery) principles to ensure reliable and well tested deployments of code into production. During development, tools are used to identify vulnerabilities within our component stack and sniff out coding errors in real time.
Physical Security	Offices on-site and off-site should be always secured to prevent unauthorised access. This can include access cards to enter buildings, a visitor sign-in/out policy and CCTV cameras.	Our offices are secured via access cards and all staff and visitors are required to sign in/out of the building. We also use CCTV security monitoring, have a paperless office policy, and any sensitive information can only be accesses by authorised persons.
Network Security	The company's network should have robust security measures and up-to-date risk and continuity plans. Network security can include firewalls, anti virus software, and intrusion detection systems.	Our secure office network operations and secure data centre operations form part of our ISO27001 accreditation and are regularly assessed.
Employee Training	Anyone employed at the company should have a good understanding of what information security policies and procedures are in place through regular training. The employees should also be practicing good security efforts, such as locking their devices, reporting phishing scams and having secure passwords.	We undertake annual mandatory training for all employees across multiple topics, including cyber security and data protection. All policies must be attested by every employee.
Compliance	The company should be up to date with relevant security regulations. Compliance with these regulations shows an active effort on the part of the business to be security conscious. These could include GDPR, ISO 27001 or Cyber Essentials Plus, amongst others.	We undertake external and internal auditing annually with the ISMS audit program to achieve an ISO 27001 certification. Additional, region-specific certifications are obtained.

Security Type	What does this mean?	At Thinkproject
Third-party risk	The business should have a vendor management program in place to ensure that third-party suppliers also follow appropriate security measures.	We have a Supplier Management Process that adheres to our ISMS requirements. This includes review of any external suppliers with our compliance team, NDAs, GDPR checks and other measures to ensure compliance with our standards. Our third-party vendors are regularly assessed to ensure they remain compliant.
Data Protection	If applicable in your location, your provider must be GDPR compliant. Furthermore, the organisation should be able to provide you with all the information about their data protection practices and how they safeguard your information.	GDPR compliance of thinkproject companies and their products is top priority External DPOs are appointed for various Thinkproject legal entities and countries, e.g. thinkproject Deutschland GmbH and thinkproject Holding GmbH. In other entities, internal data protection officers or data protection coordinators are implemented to ensure compliance with group data protection requirements Regular data protection audits are integral part of our Data Protection Management System. Mandatory annual GDPR training is in place for all our employees. We adhere to our group wide robust Data Protection Policies
Incident Response	It is important that the provider has plans in place in the event of a security breach. This could include their detection, response and recovery plans, as well as the actions taken to inform customers in such an event.	Our Incident Management Procedure is in place and regularly tested and assessed to ensure it provides prompt response to any incidents. We provide clear training for employees on reporting incidents via our whistleblower portal, and our One Trust platform.
Vulnerability Management	The provider should be regularly updating, patching and testing their software to mitigate an attacker exploiting any vulnerabilities.	As part of our secure data centre operations, we have tools in place that identify potential vulnerabilities, meaning we can act quickly to mitigate any potential threats.

Security Type	What does this mean?	At Thinkproject
Security Incident History	Enquiring about past security incidents is a good way to gauge the transparency of the organisation. They should be able to offer you their insights into the lessons learnt, how the incident was handled and what has been implemented since the event.	Any incidents are tracked with the One Trust tool. For every incident, root cause analysis and lessons learned are implemented according to our Incident Management Procedure.
Contractual Security Commitments	Contractual agreements and SLAs (Service Level Agreements) should be clear and easy to understand.	All our Thinkproject products have SLAs that can be provided on request.







Insights from the Expert

Dr. Ralf Hundhammer, CTO of Thinkproject, shares key perspectives on information security

We asked Dr. Ralf Hundhammer for his thoughts on a series of information security questions. Ralf has more than 20 years of experience in the subject and provides valuable insights.

If you were a business new to information security, where would you start when it comes to safeguarding your data and implementing an information security strategy?

Creating a security strategy sounds daunting, but like every process, it can be broken down into smaller parts that combine to work together. Firstly, it is important to take a step back and get to know your data. Understand why you have it, and why you need it. Is it necessary to have this data? Can you encrypt it? These are some questions to think about. Understanding what data your company handles will help you and your security team evaluate the associated risk and protect it in the appropriate way.

Speaking of your security team, ongoing training is crucial to keep them up to date. New threats emerge regularly, and your team need to be aware of those. Invest the energy into developing your security team, because a data breach is far more costly. This also goes for your wider workforce- the whole company should be able to assess a potential threat, whether that's through regularly simulated phishing attacks or periodic password changing. Think about your physical space too, for instance, at Thinkproject we operate on a clear desk policy and paperless offices, meaning there is less information lying around.

Once these are in place, the rest should come naturally. Create clear information security policies, practice strong authentication methods and make sure everything is kept updated. Prepare your incident response plan, get audited and build on your strong foundation of knowledge to get those accreditations that tell the customer you're a security-conscious business.

Cyberattacks continue to become more sophisticated. What do you think the biggest risk is, and how should the AECO industry tackle it?

One of the biggest concerns is the potential compromise of critical infrastructure and sensitive project data. With the widespread use of integrated systems, cloud platforms, and Internet of Things (IoT) devices, the reach of an attack has expanded massively. By combining strong technical defence with an educated workforce, organisations can effectively mitigate cyber risks and safeguard its critical assets.

Just as technology continues to evolve, unfortunately so does the sophistication of attacks. Your ISMS needs to be reviewed regularly and be flexible enough to accommodate changes as the attacks continue to advance. It's a balancing act between being ready to adapt, and sticking to a clear roadmap that your whole organisation can understand.

Organisations should prioritise collaboration and information sharing between businesses, as well as partnering with cyber security experts so that the industry can be as informed as possible. When we are all working together the risks can be mitigated, particularly with any 'lessons learned' that are valuable for other businesses to be aware of.

What best practice does Thinkproject have in place to protect the customers it works with?

Since our founding we have taken data protection very seriously. As a German-owned and Europe-based business we are extremely well versed in data protection! Our Compliance Team go to great efforts to ensure our entire workforce completes regular training on GDPR, ISMS and our contingency plans.

We pride ourselves on our robust measures to ensure the safety of data for our customers, employees and business. Our handy chart shows the measures we have in place, and how these are regularly assessed and updated.

Safety guaranteed: safeguarding your information assets

These top tips will help you shape your information security and data protection into a robust, resilient system.

Conduct Regular Risk Assessments

- Find potential vulnerabilities
- Look for any threats
- Assess and prioritise threats
- Use your findings to develop a risk management plan

Introduce Clear Security Policies

- Outline best practices
- Advise how to use the system and handle data
- Guide your employees on their responsibilities
- Review policy and procedures often

Empower Workforce with Knowledge

- Provide regular training and assessments
- Educate employees on best practices (e.g. strong passwords)
- Share your learnings from threats with employees

Use Strong Access Controls

- Ensure only authorised individuals can access the data they need to
- Set up authentication methods for extra security (e.g. Privileged Access Management)

Keep Infrastructure Up to Date

- Update and patch all your systems regularly
- Make use of firewalls to keep harm away
- Secure your networks to prevent unauthorised access

Top Tips

Tips to help continued

Comply with Regulations

Applicable regulators in your field will be a helping hand to ensuring best practice at your own organisation

GDFR, CCPA, etc, will have the most up-to-date advice to secure your network

Encrypt Sensitive Data

Even of data is compromised, when encrypted it cannot be read

GDPR policies should include encryption of data

Make an Incident Response Plan

Develop and test your response plan regularly to ensure the most up to date factors are included

Define roles and responsibilities as well as clear communication channels

Collaborate and Share with Other Org's

Information sharing with your peers is a good way to understand the current attack landscape

Sharing best practices ensures everyone can stay protected

Access Supply Chain and Vendors Often

Your software and cloud providers should have their own policies to protect your organisation's data

These should be up to your own security standards

Information Security trends, every business should know in 2024 and beyond

In an ever-changing and increasingly digital landscape, things move incredibly fast. When it comes to your information security, what may have been gold standard a couple of years ago can quickly go out of date. This is why it's important to refresh yourself with best practices regularly to make sure your business is protecting itself the best in can.

Find out our top trends below.

Zero-Trust Security:

Your website going offline due to attacks is one thing, but when your whole system is compromised by a cyber threat, that is a major disaster for your company. Zero-trust security is an approach to network safety that assumes all traffic is potentially hostile, requiring verification before granting access, therefore making it more difficult for cyber threats to reach their intended targets.

Multi-Factor Authentication (MFA):

MFA can drastically reduce the risk of accounts becoming compromised and leading to security breaches. By requiring more than one form of authentication (for example, a password and then a code sent to the corresponding mobile device) a potential hacker will have a much more difficult time in gaining access to your company's data.

AI and Machine Learning:

Artificial Intelligence (AI) and Machine Learning (ML) now offer ways to boost security. Both AI and ML have been used to analyse massive amounts of data in real-time , analysing trends and identifying unusual behaviour or activity.

Investment in Cyber Security Talent:

With the advent of cyber security being relatively new, globally we are going through a cyber security talent shortage, meaning if a business wants a dedicated professional on the team to cover their information security, they will need to invest in training, development and upskilling existing staff. Alongside this, cyber security apprenticeships are growing in popularity, with new talent looking for companies to flourish in.

Data Privacy Regulations:

With the increasing emphasis on data privacy, businesses need to ensure that they comply with relevant regulations, such as GDPR. This involves implementing appropriate security measures, such as data encryption and access controls, and ensuring that they have policies and procedures in place to protect the privacy of their customers' data.

Be proactive to overcome security threats

In conclusion, today's fast-paced digital landscape means businesses must be proactive in safeguarding theirs and their customers information from cyber threats. As we have read, the consequences of data breaches and attacks are often devastating to business and individuals.

By adopting a proactive mindset alongside a comprehensive security policy, businesses can identify vulnerabilities, assess risks, and implement robust security measures that (under regular maintenance) can serve the business for years to come. Alongside this, staying updated on security trends and complying with regulations are crucial components of a proactive approach to information security and are positive signs to look out for in any business, whether you are the customer or the provider.

To learn more about how Thinkproject combines innovative construction software solutions with the gold-standard of security, visit our Trust Centre.

Thinkproject Trust Centre

thínkproject

Thinkproject is Europe's leading SaaS provider for Common Data Environment, Asset, BIM and Field Management, and Project Controlling. Thinkproject has been digitising construction companies, builders, project managers and planners for more than 20 years with powerful, flexible technology in combination with consulting expertise from knowledge of complex large-scale projects.

With 650+ employees worldwide, Thinkproject offers digital solutions that cover the entire life cycle of a construction project.

75000
PROJECTS

3250
CUSTOMERS

300000
USERS, IN OVER...

60
COUNTRIES

650+
CUSTOMER-ORIENTATED EMPLOYEES

23
OFFICES

Thinkproject.com