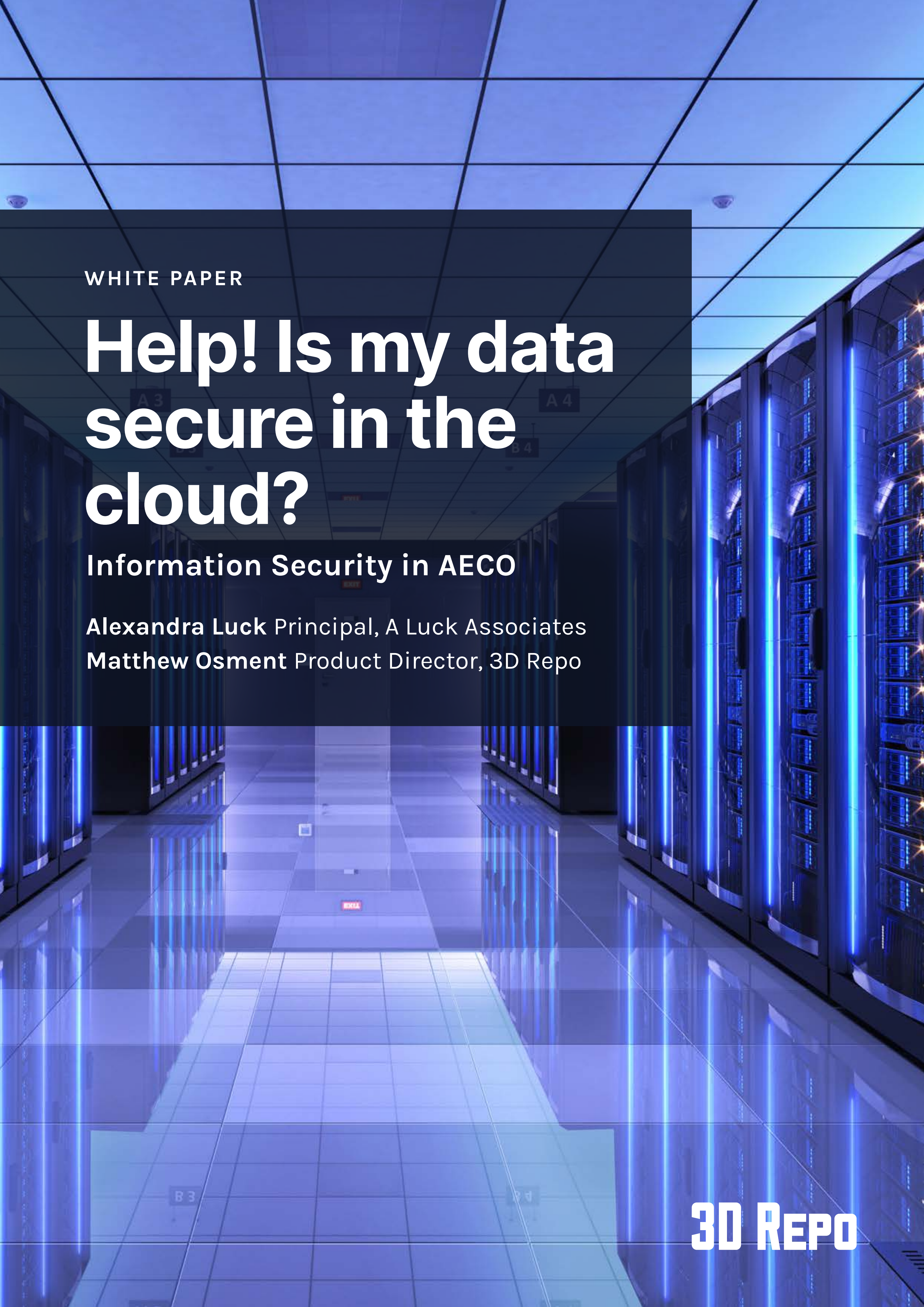


WHITE PAPER

Help! Is my data secure in the cloud?

Information Security in AECO

Alexandra Luck Principal, A Luck Associates
Matthew Osment Product Director, 3D Repo

3D Repo

Foreword

Many will agree that these days, data is the new oil. But if that was the case, why would anyone allow unscrupulous managers of their oil fields to siphon away barrels and barrels of crude in order to refine and sell it on? Even more worryingly, the oil magnates would willingly sign up to such a deal because that is what the Terms & Conditions said, which everyone is thoroughly reading through before accepting...

In the physical world, this analogy clearly makes no sense, yet in the virtual world that is exactly what happens every single time we sign up for a new cloud service. However, as they say in Silicon Valley, "there is no cloud, it's just someone else's computer". Such a realisation, therefore, poses huge ramifications especially in the AEC sector. And we are not necessarily talking about GDPR responsibilities relating to personal data. We are talking about 2D drawings and 3D models of national and even international significance that are accurate down to the millimetre!

In this whitepaper, we therefore draw upon our own experiences of handling some of the most security minded projects such as national parliaments and nuclear power stations in order to provide a checklist for BIM managers, IT procurers, and project directors to follow. The hope is that this document really makes you stop and think twice about where you upload your data. The message is clear, simply ticking the ISO 27001 supplier checkbox should never be enough to comply with your clients' requirements on its own.

Dr Jozef Dobоš CEng
Founder and CEO, 3D Repo

Under attack!

Data breaches in the construction sector are rising exponentially. Data from risk consulting firm Kroll[1] shows that there was an 800% increase in breaches in 2020 compared to 2019. And an analysis of 1,200 ransomware attacks between 2020 and 2021 by encryption software company Nordlocker[2] found that construction was the industry most attacked.

The conflict in Ukraine further increases risk. The National Cyber Security Centre (NCSC), part of Government Communications Headquarters (GCHQ) has called on businesses to bolster their online defences. Wiper malware, which can erase data from hard drives, has already been used against Ukraine[3].

There are several reasons why attacks on construction companies have been rising so steeply. First, we were starting from a low base, since historically cyber-attacks on construction companies have been relatively few. Secondly, the industry's use of digital and online tools has risen dramatically, with uptake accelerated by the pandemic. And finally, there have been a series of high-profile hits on large construction companies, highlighting potential gains for other would-be hackers and ransom-takers.

Cloud-based platforms for construction projects have really come into their own during the COVID-19 pandemic, allowing teams of people located remotely from each other to collaborate effectively. But users of such systems must be aware of the potential security risks attached to these platforms and protect themselves accordingly. Rules about data ownership and access vary from country to country – and from provider to provider.

"Some organisations have always had to be very aware of security threats such as terrorism and espionage but security threats also include commercial espionage, organised crime, activists, lone actors, hackers and malicious insiders. Further, the increasing use of, and dependence on, information and communications technologies means all organisations need to address inherent vulnerability issues," says security adviser Alexandra Luck of A Luck Associates. "The greatest challenge is people not being aware of how insufficient information security can impact their organisation, projects and built assets."

What are the security risks?

There are several motivations for seeking to obtain unauthorised access to information: holding data to ransom, stealing personal details, making a political point and state-sponsored attacks.

With high-value payments being made electronically across projects, theft of money is a common problem in construction too. Intellectual and commercial property can also be valuable, with threat actors potentially seeking to steal tender information on international projects.

Some data is insecure due to internal inactions, rather than external actions: lapses, oversights or a lack of robust procedures. Some companies unknowingly create security risks because they haven't understood the access and use rights for the data storage location they have chosen. They may even be unaware of where all their data is stored – which means that if they suffer a security breach, reacting and recovering will be more difficult.

One important fact to grasp is that all clouds are not created equal. At one end of the scale are public clouds, where the provider determines all the security measures and the user has no power to change them. It's important to read the small print; it could be that your construction cloud platform provider has the right to move your data to or through another country without notifying you in advance.

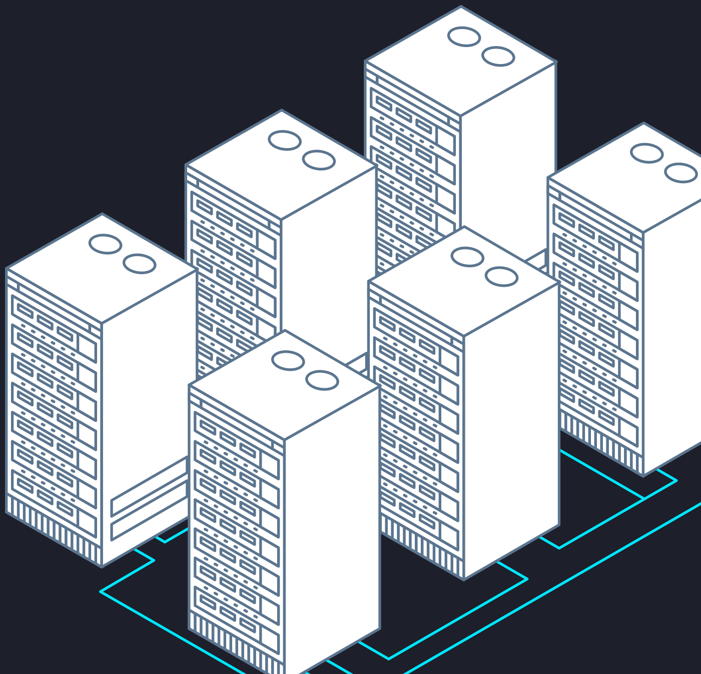
At the other end of the cloud spectrum are private secure systems, where the user procures the security measures they require, usually with much more segregation and protection of the data. The middle ground is hybrid clouds, where organisations with similar security requirements – such as government departments – share cloud systems.

"If you have sensitive information, you need to think about how you manage and segregate it," says Luck. "Think about what information you want to protect and what your risk appetite is."

Technology is developing so quickly that over the lifetime of a built asset, or even over the lifetime of a construction project, data can become accessible to less sophisticated threat actors.

For example, there have been several recent incidents where BLOBs - binary large objects, such as video files or images - have been left insecure, giving people access to the information in them. In one instance, personal data about participants of a webinar was put into a BLOB which was effectively in a public cloud. [4]

"With any advance in technology, we need to understand how information is being used.
We may be bringing information together and combining it, sometimes in a way we would not have thought about," says Luck. "We need to make proactive decisions, rather than have security as an afterthought. Retro-fitting security measures is likely to more expensive and less effective than building in appropriate controls from the beginning."



What should be protected?

It is tempting to think that all data should be securely locked away behind high and impenetrable walls. However, the reality is that only a small proportion of any company's data will be sensitive.

"Even for highly secure buildings, the majority of project or asset information may not be sensitive," says Luck. "But identifying what is critical and applying appropriate and proportionate security controls in relation to that is essential."

Clearly, some construction projects – such as the defence sector or nuclear power plants - involve more sensitive information than others. However, many buildings and parts of our infrastructure will contain elements which help to ensure the safety and security of the assets themselves, their users or the services the assets provide. Sensitive information relating to these aspects should therefore be appropriately protected, explains Luck.

Consideration must also be given to the information which projects hold about sensitive assets belonging to others. Luck has seen construction plans which map and label the presence of "nationally critical infrastructure".

Sensitive data does not just relate to information about built assets, organisations are likely to want to protect their intellectual property (IP) using a similar approach. Access to sensitive information should be limited to those who have a genuine need to know, with access removed when that need no longer exists, says Luck.

In addition, BIM and collaborative platforms have muddied the water in terms of IP. While some client organisations might say that anything developed as part of the programme is their IP, others might say that if an organisation has brought IP to the programme but has not developed it as a result of being paid to do work, it should be retained by them.

It is important that these boundaries are agreed and set as early as possible, before contracts are signed, to avoid disputes down the line (see section, Who owns your data?).

Where is your data?

Storing data 'in the cloud' sounds like information is close at hand, hovering somewhere above our heads. In practice, this can be far from the case. 'The cloud' is a data storage centre, located somewhere else, accessed over the internet and maintained by a third party.

Data residency - where the data is physically stored - is important because laws governing data vary from country to country. It may be that a company is compelled by law to store certain information, such as customers' personal details, in their home country. Or a business may want to store information in a country where tax regulations are favourable.

The other point to note is that data may not take a direct route from A to B. Internet networking systems are designed to send data on the best route at the time which may mean that your data is crossing over borders into other countries, and back again – so-called boomerang routes.

"You need to know the locations at which your information is stored, processed and managed to understand the legal circumstances under which it could be accessed by others without your consent," advises Luck.

It is also worth noting that some countries' access to data extends far beyond their borders. For instance, amendments made in 2014 to the US's Stored Communications Act mean that a company's data is subject to US law enforcement warrants, even if it is stored elsewhere. This was confirmed in a case involving emails allegedly linked to drug trafficking, which were stored by Microsoft in Dublin[5].

Case Study: Canadian Parliament, Canadian data

In Ottowa, Canada, a 10-year programme to update the Canadian Parliament complex is underway. Originally built in 1860 and reconstructed in 1916 following a fire, the complex will be refurbished and remodelled to create modern and accessible spaces.

CENTRUS, an HOK and WSP-led team, is working on the design of the Parliament's central block which houses Canada's Senate, House of Commons and Library of Parliament. CENTRUS is using 3D Repo as an advanced versioning system to track and store all the changes and evolutions to the 3D design.

One of the challenges for any company looking to use cloud-based collaboration tools in Canada is that the Canadian Government mandates that all information must be stored geographically within Canada's borders. 3D Repo was able to rise to this challenge as its software is easily deployable to any cloud infrastructure, or on-premise, allowing it to quickly supply service wherever data residency is required.

How can I protect my data?

The Centre for the Protection of National Infrastructure (CPNI) sets out 20 principles for senior executives in its Passport to Good Security[6], the first of which is good governance: identifying who is accountable for security at the board level and establishing clear reporting lines between them and those in the organisation who are involved in security.

“To create a security-minded approach requires good personnel, physical and cyber security, with good governance which includes accountability and responsibility for security to pull those three different strands together,” says Luck.

The first step in an information security strategy might be to segregate information in terms of its value and sensitivity. Perhaps only a small number of people within an organisation would have access to the most sensitive of data. It would also make sense to tightly control where that data goes – and how it travels.

Encryption is important for sensitive information. Note that encryption of information, while it is at rest, is as important as encryption during transit; something that some organisations and software providers overlook.

A good place to start when checking on your cloud service provider’s security approach is the National Cyber Security Centre (NCSC)’s 14 principles. The NCSC, which is part of the Government Communications Headquarters (GCHQ) published the 14 steps or principles in 2016. They align with ISO 27017: 2015 Information technology — Security techniques — Code of practice for information security controls based on ISO 27002 for cloud services.

Who owns your data?

With the rise of collaborative practices – and platforms that enable them – has come the question of who owns the data? Is it the project owner, the company that created the data or the main contractor, who is often the one procuring the cloud-based platform?

The answer should lie in the contracts. The client should set down what information they are procuring, in what form and who has responsibilities for it – in terms of its hygiene and its maintenance. In practice, clients are still getting up to speed with this, which leaves grey areas and risk.

What users of cloud-based platforms may not be aware of is that the platform provider could be using the data in their cloud. It is vital to read the terms and conditions associated with the platform which will set down not only who owns the data but also what the service provider can do with it. The small print may well come as a surprise.

With the rise of Artificial Intelligence (AI) and machine learning, data that can be accessed and used to train algorithms becomes even more useful. Last year, a judge ruled that a machine-learning programming assistant, GitHub Copilot, could use code hosted on its GitHub platform[7]. It’s not a big leap to think of similar AI opportunities in the construction sector.

NCSC's 14 steps to cloud security[8]

1. **Data in transit protection** - user data transiting networks should be adequately protected against tampering and eavesdropping.
2. **Asset protection and resilience** - User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
3. **Separation between users** - a malicious or compromised user of the service should not be able to affect the service or data of another.
4. **Governance framework** - the service provider should have a security governance framework that coordinates and directs its management of the service and information within it.
5. **Operational security** - the service needs to be operated and managed securely in order to impede, detect or prevent attacks.
6. **Personnel security** - where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness.
7. **Secure development** - services should be designed and developed to identify and mitigate threats to their security.
8. **Supply chain security** - the service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.
9. **Secure user management** - your provider should make the tools available for you to securely manage your use of their service.
10. **Identity and authentication** - all access to service interfaces should be constrained to authenticated and authorised individuals.
11. **External interface protection** - all external or less trusted interfaces of the service should be identified and appropriately defended.
12. **Secure service administration** - systems used for administration of a cloud service will have highly privileged access to that service.
13. **Audit information for users** - You should be provided with the audit records needed to monitor access to your service and the data held within it.
14. **Secure use of the service** - the security of cloud services and the data held within them can be undermined if you use the service poorly.

Should I vet my employees?

As outlined above, humans are just as important as software tools when it comes to creating a security-minded organisation. The first step is raising awareness, by providing information and training. If people understand why rules and procedures are in place, they are more likely to follow them.

Reinforce everyday good practice: don't open emails that could be suspect, don't say yes to every LinkedIn request that comes along. Employees should also be trained in human factors too, such as how to notice if a colleague is under stress or behaving differently. Vulnerable employees can be a good way in for threat actors. If someone is struggling financially, for instance, they could be more likely to succumb to financial incentives.

It is also important to remind employees that physical security is as important as cyber security. If someone can walk into a site office and help themselves to a phone or PC unchecked, then an organisation's efforts on ensuring information security may go to waste.

However, security protocols and processes should be appropriate and proportionate. Overly complex security measures make it difficult for people to do their job and could lead to employees circumventing or ignoring systems. Again, think of segregating data so that only the most sensitive is highly protected, and consider limiting access to that data and then providing additional training and checks for those with access.

When it comes to cloud-based platforms, it is important to be security-minded about who has access to what data – within your own organisation and within your supply chain companies. This should be agreed contractually at an early stage, but then it is important to keep abreast of access requirements and controls as parties and individuals leave and join the project.

Standards for the security minded

BS EN ISO 19650-5:2020: Organisation and digitisation of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling. Security-minded approach to information management.

ISO/IEC 27001:2013 (or ISO 27001): Information technology — Security techniques — Information security management systems — Requirements

Is my supply chain secure?

What security breaches have revealed very clearly over recent years is that organisations really are only as strong as the weakest link in their supply chain – and that threat actors will find those weak spots and exploit them.

"It is often referred to as the soft underbelly: the organisation that has the poorest security is likely to be targeted," says Luck. "The more you share information across organisations, the more you have to ask: how do we collaborate in a security minded way?"

While construction clients should be setting standards for information security and behaviour in their contracts, organisations in the supply chain also have a role to play in improving security, says Luck.

"Since they are going to be sharing information, the supply chain can ask for the kind of security-minded approach that they need too," she says. "People should feel confident to discuss these issues and highlight any concerns. These conversations should be had as early as possible and an approach agreed upon, implemented and monitored to ensure its effectiveness. However, it's never too late to think about security – a security-minded approach can be adopted in relation to projects that are already in-train or in the management of existing assets."

Case Study: Hinkley Point C - encryption secured data

The construction of the UK's £20bn-plus Hinkley Point C power station is well advanced. The next-generation nuclear plant will provide lower-carbon energy for 6 million homes when it begins operation in 2026.

SNC-Lavalin Group company, Atkins, has designed the technical galleries for the new station; underground tunnels which connect structures above ground. Atkins is using 3D Repo to federate models created in different software packages, allowing it to detect changes and manage design issues.

Clearly, data security is of high importance on projects such as Hinkley Point C. With 3D Repo, data is fully encrypted whilst stored and in transit, which makes it secure. 3D Repo is also ISO 27001 Information Security Management certified by BSI.

What happens after handover?

In an ideal world, data gathered during the design and construction phases would flow seamlessly on to be used in an asset's operational phase.

In many cases, historic project information may not even be accessible, as licences to use cloud-based platforms expire, entities such as joint-venture contractors disband or companies are acquired or disappear. The NCSC advises in its Cyber security for construction businesses guide[9], published in February 2022, that companies should identify what their business-critical data is and back it up religiously.

Just as a lack of interoperability between software packages can be a problem during the construction phase, it can also be problematic as assets move into operation. This can also mean that data that has been stored on a cloud platform is no longer accessible down the line.

However, continuity of information flow will become a must. One of the requirements that came out of the Hackett Review of the Grenfell Fire is that information relating to high-rise buildings should be available and accessible to building occupiers, owners and others. This idea of a 'Golden Thread' of information is now part of the Building Safety Bill and is expected to spread into all sectors of the industry as governance around information management tightens up.

"The Golden Thread relates to both the information about a building that allows someone to understand a building and keep it safe, and the information management to ensure the information is accurate, easily understandable, can be accessed by those who need it and is up to date. While the golden thread specifically relates to information on building safety, the key principles relating to information management, and implementing these in a security-minded way, are good practice for any organisation that is generating, processing, sharing and storing information," concludes Luck.

Cyber Essentials

3D Repo maintains the Cyber Essentials Certificate of Assurance, providing its customers with an additional layer of confidence in its security measures.

Cyber Essentials is a Government-backed certification scheme that demonstrates that an organisation has the right defences in place to protect itself against cyber-attack. Companies need to have Cyber Essentials certification to bid for certain central Government contracts[10].

Launched in 2014, Cyber Essentials sets down five basic technical controls which organisations must have in place to protect themselves against security threats: boundary firewalls and internet gateways; secure configuration; access control; malware protection; and patch management[11].

To gain certification, companies must complete an online self-assessment questionnaire, supported by a board member who signs a declaration to say that the answers are true.

3D Repo's security checklist for selecting cloud systems

■ Data access

- Who has access to the data?
- Who are the developers and where are they based?
- What protections are in place for those with access?

■ Data storage

- Where is the data physically stored? How is your data stored?
- How is the data encrypted?

■ Data use

- How can the provider use your data? Who owns the data and can it be sold?
- Can data be mined and for what purpose?

■ Data removal

- How is data deleted?
- How is data backed up and for how long?
- Can data be easily accessed and moved to another service?

3D Repo's approach to information security

Where is data stored by 3D Repo?

3D Repo's cloud storage sits on top of Amazon's public Cloud called Amazon Web Services (AWS). The AWS Cloud has data storage facilities in 26 geographic regions around the world. This means that for almost every project that uses 3D Repo, data can be stored within that country's boundaries.

What can 3D Repo do with its user's data?

3D Repo does not own any of its users' data, nor does it have the right to reproduce some of its users' data – unlike some of its competitors.

Are the data centres physically secure?

Yes. Amazon operates a high level of physical security at its data centres. As Amazon is responsible for running large parts of 'the cloud' they have implemented many security controls to protect themselves and their clients

Does 3D Repo use encryption?

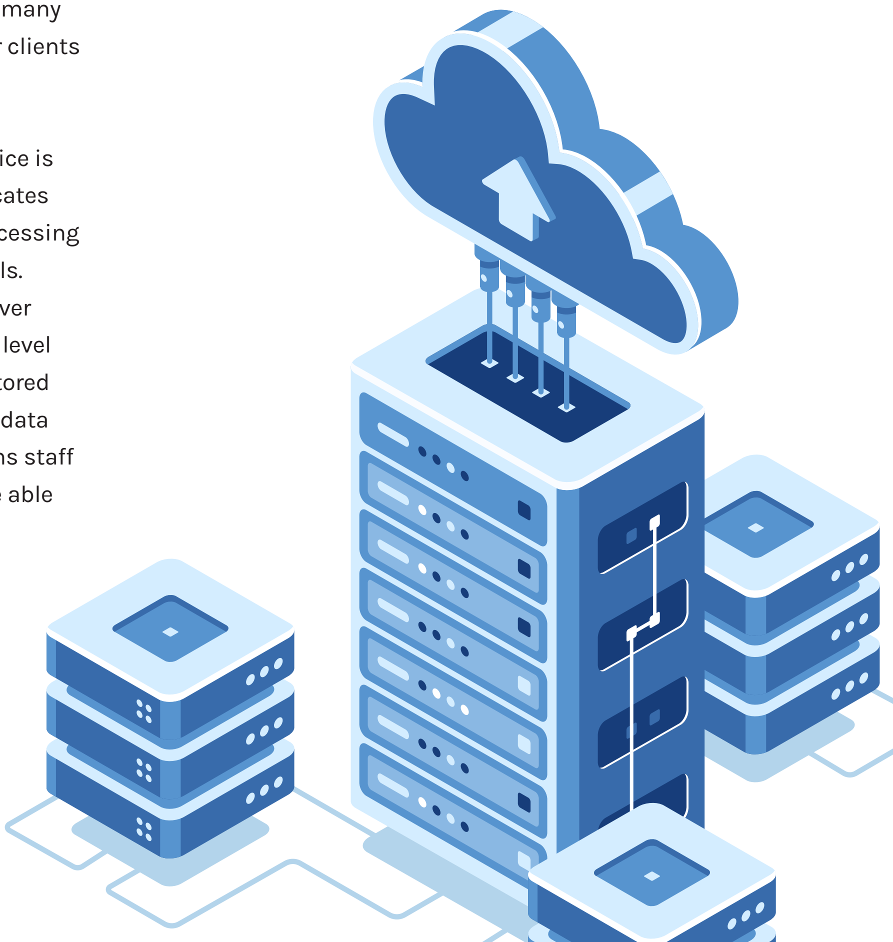
Yes, at all layers. An initial connection to the service is secured via 2048 Bit Extended Validation Certificates which means users can confirm that they are accessing a 3D Repo service before entering their credentials. Once logged in, all communications take place over HTTPS-secured connections, providing the same level of protection as internet banking. Once data is stored on its platform, is it encrypted again so that the 'data at rest' is encrypted with keys that only operations staff have access to. This means that if someone were able to break into the data centre and remove the servers running the platform, user data would not be accessible.

Will data be accessible in the future?

Yes. 3D Repo is also open source, which means its users can inspect the operating code and ensure that they are happy with the operating principles. It also means that the software can be transferred to databases or software for asset management and can be downloaded and operated in 10, 20, or even 100 years' time.

What cyber security certification does 3D Repo have?

3D Repo was one of the first BIM platforms to become ISO 9001 and ISO 27001 certified through BSI in 2019. In 2021, it achieved the UK Government's Cyber Essentials Certificate of Assurance.



References

1. https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021
2. https://nordlocker.com/recent-ransomware-attacks/
3. https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences#:~:text=Following%20Russia's%20unprovoked%2C%20premeditated%20attack,the%20cyber%20threat%20is%20heightened.
4. 'Blob' at DataBreaches.net
5. Data residency is security theatre | Sean Boots (sboots.ca)
6. https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf
7. https://fossa.com/blog/analyzing-legal-implications-github-copilot/
8. https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
9. https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses
10. https://www.ncsc.gov.uk/cyberessentials/overview
11. https://3drepo.com/mitigating-online-risk-with-robust-cyber-security-systems/

Alexandra Luck
Principal, A Luck Associates

Alexandra Luck is a Chartered Engineer, a Fellow of the Institution of Civil Engineers, a Fellow of the Chartered Institution of Highways and Transportation, and a Member of the Register of Security Engineers and Specialists. She has authored, and been involved in the production of, standards in the UK and internationally in relation to the implementation of security and security-minded approaches as well as authoring a number of supporting articles, documentation and guidance material. She has provided advice on the implementation of security-minded approaches to digital engineering within a number of projects across a range of sectors, and comprising both buildings and infrastructure. She also has extensive experience in the development, implementation, management and auditing of proportionate and structured management systems, policies and processes and has undertaken forensic investigation and analysis of incidents, previously frequently acting as an expert witness.

Matthew Osment
Product Director

Matthew is the Product Director at 3D Repo. Previously he has been consulting in the construction industry in various forms for the past 5 years, working predominantly with Main Contractors focusing on innovation and efficiency in Planning and Commercial activities, with a focus on BIM. Prior to that Matthew was a Product Design Engineer in the transportation and consumer goods space, learning about the power of parametric modelling, 3D as a communication tool and Total Quality Management.

3D Repo

3drepo.com