IMPACT REPORT: Cyber Security

SHERIFF

CYBER CRIME IS SURGING IN THE UK

BUSINESSES AFFECTED BY CYBER-ATTACKS

ALL BUSINESSES	50%
UK CONSTRUCTION FIRMS*	58%
MEDIUM-SIZED BUSINESSES	70%
LARGE BUSINESSES	74%

*Data from 2023/ All other data from 2024

MOST COMMON ATTACKS

Phishing (fraudulent emails pretending to be legitimate to trick users)

Impersonation (scammers posing as trusted contacts, often via email)

Viruses/malware (malicious software that harms devices or steals data)

CYBER ESSENTIALS CERTIFICATION

12%

UK subcontractors certified

Only 12% of UK subcontractors have this UK government-backed scheme to prove basic cybersecurity protections

AVERAGE COST OF A BREACH

ALL BUSINESSES	£1,205
MEDIUM/LARGE BUSINESSES	£10,830

WHY CYBER SECURITY MATTERS

Cyber security threats are escalating across the UK, with more than half of all businesses reporting a breach in 2024. These breaches (unauthorised attempts to steal, damage or disrupt data and systems) are even more common among medium-sized businesses (70%) and large organisations (74%).

High-profile incidents at well-known names such as **Marks & Spencer, Co-op and Harrods** have shown that even the most established brands are vulnerable – with attacks forcing them to suspend online operations.

This surge in activity is a clear signal: cyber-crime is happening right now, and it can affect any organisation, regardless of size or sector.

WHY CYBER SECURITY MATTERS IN CONSTRUCTION

Construction companies handle highly sensitive information every single day – from project files and client contracts to design drawings and financial data. This makes the sector a prime target for cyber threat actors and, when a data breach occurs, the consequences can be severe:

Operational disruption

A single incident can delay or halt projects entirely and trigger financial penalties.

Financial losses

In 2022, the UK construction sector lost **£50.3M to invoice fraud** (where scammers fake invoices to redirect payments). **GDPR fines** (penalties under UK/ EU data law) can reach up to 4% of a corporation’s global turnover (depending on the severity of the breach).

WHY CYBER SECURITY MATTERS IN CONSTRUCTION

Higher overheads

Cyber insurance becomes costlier without basic protections.

Reputational damage

A security breach can harm a company’s reputation for years, risking the ability to secure future work and partnerships.

Exclusion from top clients

Tier 1 contractors and government bodies now often require Cyber Essentials certification before subcontractors can be considered.

A robust approach to cyber security is no longer optional – it is essential for protecting data, maintaining operations and securing high-value contracts.

OUR APPROACH TO KEEPING DATA SECURE

Understanding the problem…

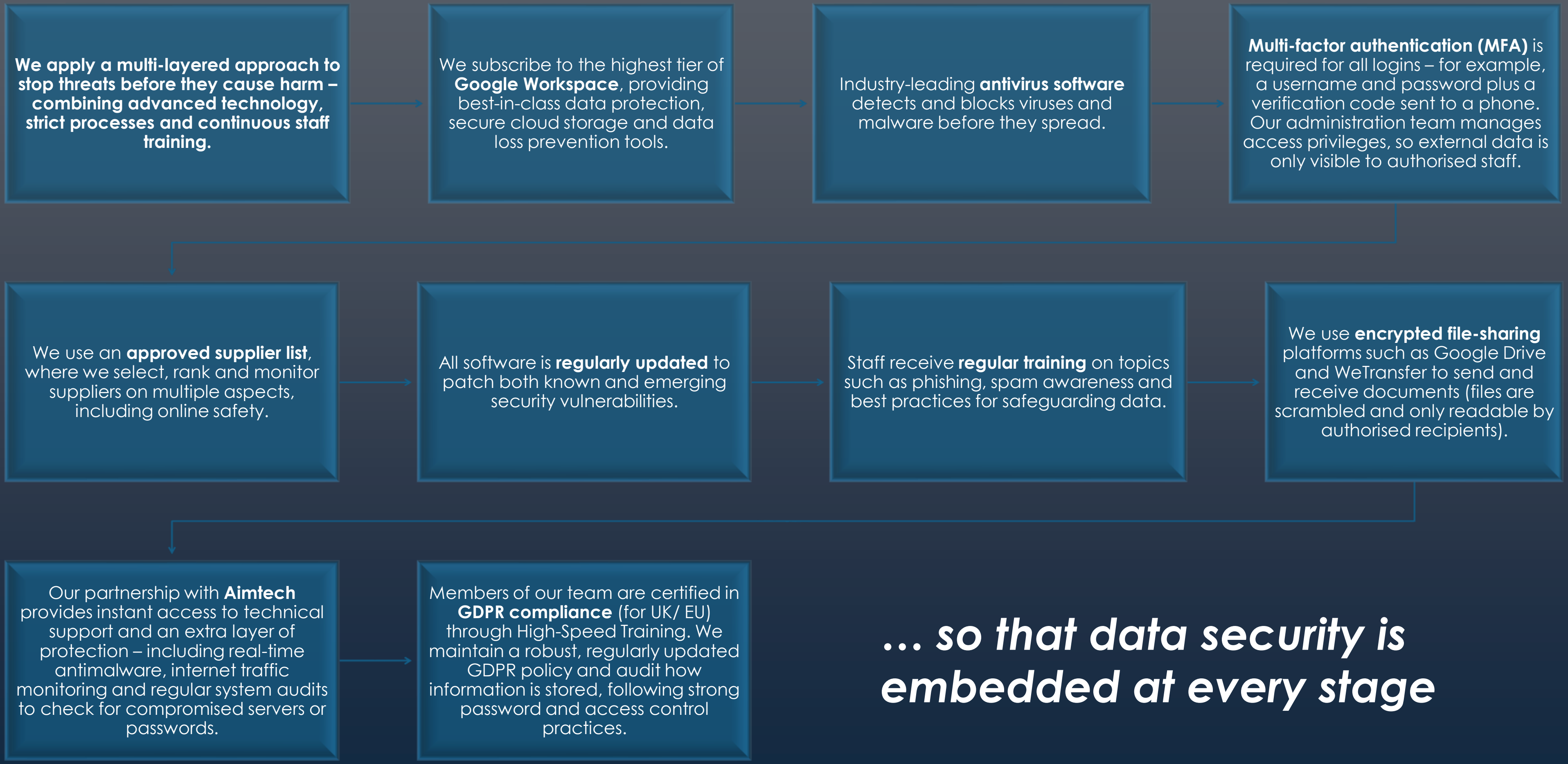
At Sheriff Construction, we have analysed how cyber-attacks are targeting the construction industry and identified the three most common exploitation routes used by hackers and fraudsters:

- **Payment deception** – Fraudsters impersonate suppliers or clients to redirect legitimate payments into their own bank accounts.
- **Logins** – Shared accounts, outdated software or unsecured devices can provide easy entry points for attackers.
- **Phishing** – Fake emails (e.g. posing as project managers) are used to trick recipients into revealing login credentials or to spread malicious software.

By understanding these high-risk areas, we can take targeted action to block the most likely threats before they cause disruption.

OUR APPROACH TO KEEPING DATA SECURE

Preventing and protecting against threats…



We apply a multi-layered approach to stop threats before they cause harm – combining advanced technology, strict processes and continuous staff training.

We subscribe to the highest tier of **Google Workspace**, providing best-in-class data protection, secure cloud storage and data loss prevention tools.

Industry-leading **antivirus software** detects and blocks viruses and malware before they spread.

Multi-factor authentication (MFA) is required for all logins – for example, a username and password plus a verification code sent to a phone. Our administration team manages access privileges, so external data is only visible to authorised staff.

We use an **approved supplier list**, where we select, rank and monitor suppliers on multiple aspects, including online safety.

All software is **regularly updated** to patch both known and emerging security vulnerabilities.

Staff receive **regular training** on topics such as phishing, spam awareness and best practices for safeguarding data.

We use **encrypted file-sharing** platforms such as Google Drive and WeTransfer to send and receive documents (files are scrambled and only readable by authorised recipients).

Our partnership with **Aimtech** provides instant access to technical support and an extra layer of protection – including real-time antimalware, internet traffic monitoring and regular system audits to check for compromised servers or passwords.

Members of our team are certified in **GDPR compliance** (for UK/ EU) through High-Speed Training. We maintain a robust, regularly updated GDPR policy and audit how information is stored, following strong password and access control practices.

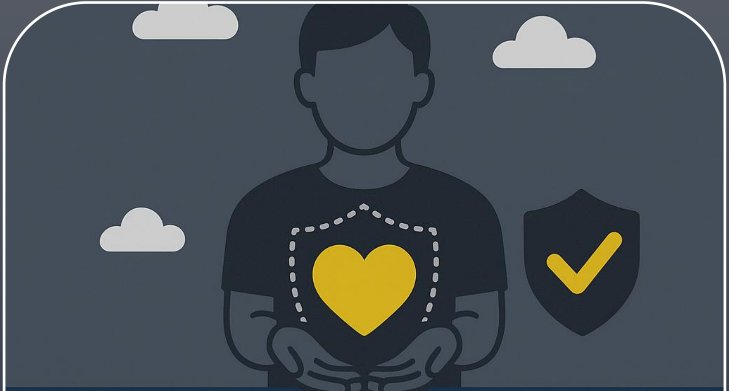
… so that data security is embedded at every stage

DELIVERING FOR OUR CLIENTS

Our cyber security measures are designed to protect information, maintain operational continuity and give clients complete confidence in how their data is handled. We focus on three core outcomes:

UNINTERRUPTED PROJECTS

Robust systems and proactive monitoring help prevent cyber incidents from disrupting schedules or causing costly downtime.

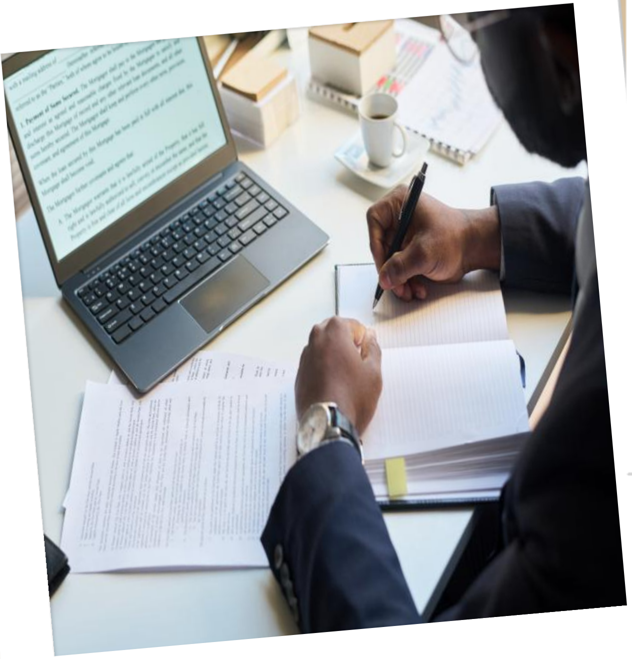


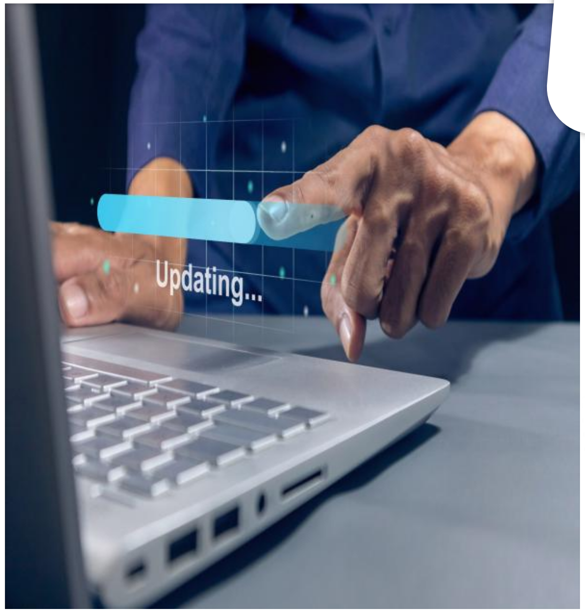
PEACE OF MIND

Clients know their information is stored, transmitted and managed securely, helping to build long-term trust and reducing stress for all parties.

COMPLIANCE ASSURANCE

Our data protection processes align with the requirements of government bodies and top-tier contractors, especially around confidentiality and the secure handling of sensitive information.





Keeping our cyber-security in top shape!

CASE STUDY:
ATTACK ON INTERSERVE (2020)

WHAT HAPPENED?

In Spring 2020, Interserve experienced a severe cyberattack that exposed the personal data of up to **113,000 current and former employees** – including bank details, National Insurance numbers and special category information such as ethnic origin, religion, disabilities, sexual orientation and health records.

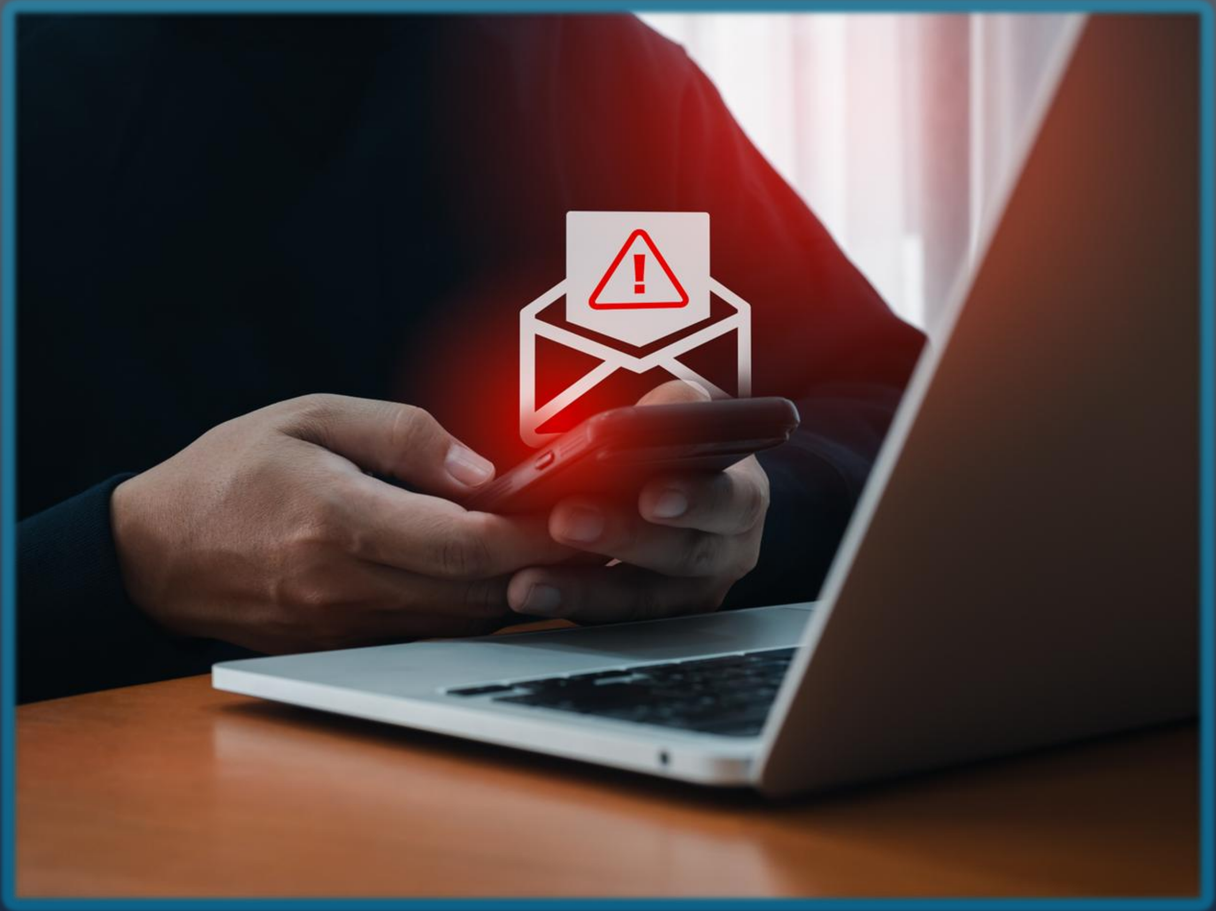
The attackers successfully uninstalled antivirus software, compromised 283 systems and 16 accounts, and encrypted four HR databases, rendering them inaccessible.

CASE STUDY:
ATTACK ON INTERSERVE (2020)

WHAT WENT WRONG?

An investigation by the UK's data watchdog, the Information Commissioner's Office (ICO) found several key failings:

- Poor training was a primary factor. The incident began in May 2020 when a phishing email was forwarded and acted upon, triggering the installation of malware.
- Although antivirus software detected the threat, no follow-up investigation took place, allowing attackers to maintain access.
- Outdated and unsupported software (with no security updates) left systems vulnerable.
- There were no adequate risk assessments or incident-response protocols.



CASE STUDY:
ATTACK ON INTERSERVE (2020)

THE OUTCOME

- ICO issued a £4.4m fine.
- The total cost to Interserve exceeded £11 million, including £7 million in professional adviser fees.
- The UK Information Commissioner, John Edwards, concluded that ***"the biggest cyber risk is complacency, not hackers."***

While the company avoided long-term operational damage, the breach could have been prevented through basic protections – including better staff training, regular system updates, phishing drills and a robust incident response plan.

WHAT'S NEXT?

Cyber-crime is always evolving so it's our job to stay ahead of that threat. We have two key focus areas – building on our existing protective measures and going further with our learning and accreditations.

Strengthening everyday protection

We will continue deploying safeguards that directly address the most common attack routes in construction, including:

- Multi-factor authentication for all payment-related processes, combined with using an approved supplier list to reduce payment fraud risk.
- Regular staff training to help identify and report phishing attempts quickly.
- Secure, encrypted platforms for all document sharing.

These measures will help ensure our projects remain seamless, compliant and trusted by clients.

WHAT’S NEXT?

Pursuing higher certifications

To further demonstrate our commitment to security further, we are working with **Aimtech** to achieve:

- **Cyber Essentials Plus** – An advanced government-backed certification that includes independent technical testing to verify that our protections are correctly implemented, systems are compliant and all networks and devices are free from vulnerabilities.
- **Tailored cyber insurance** – Ensuring we have protection that addresses the unique cyber risks faced by the construction sector.
- **ISO 27001 alignment** – Led by our in-house security champion, this will help us establish, maintain and continually improve a robust information security management system in line with international best practice.

Thank you for reviewing our Impact Report and joining us in promoting cyber security in construction.

We value your feedback

Your insights and feedback help us improve our cyber security policies and practices. Reach out via email, phone or post for any questions or feedback regarding this impact report.

August 2025

GET IN TOUCH

Sheriff Construction, 61b Runfold Avenue, Luton LU3 2EJ

info@sheriffconstruction.co.uk

01582 591908

sheriffconstruction.co.uk

SHERIFF