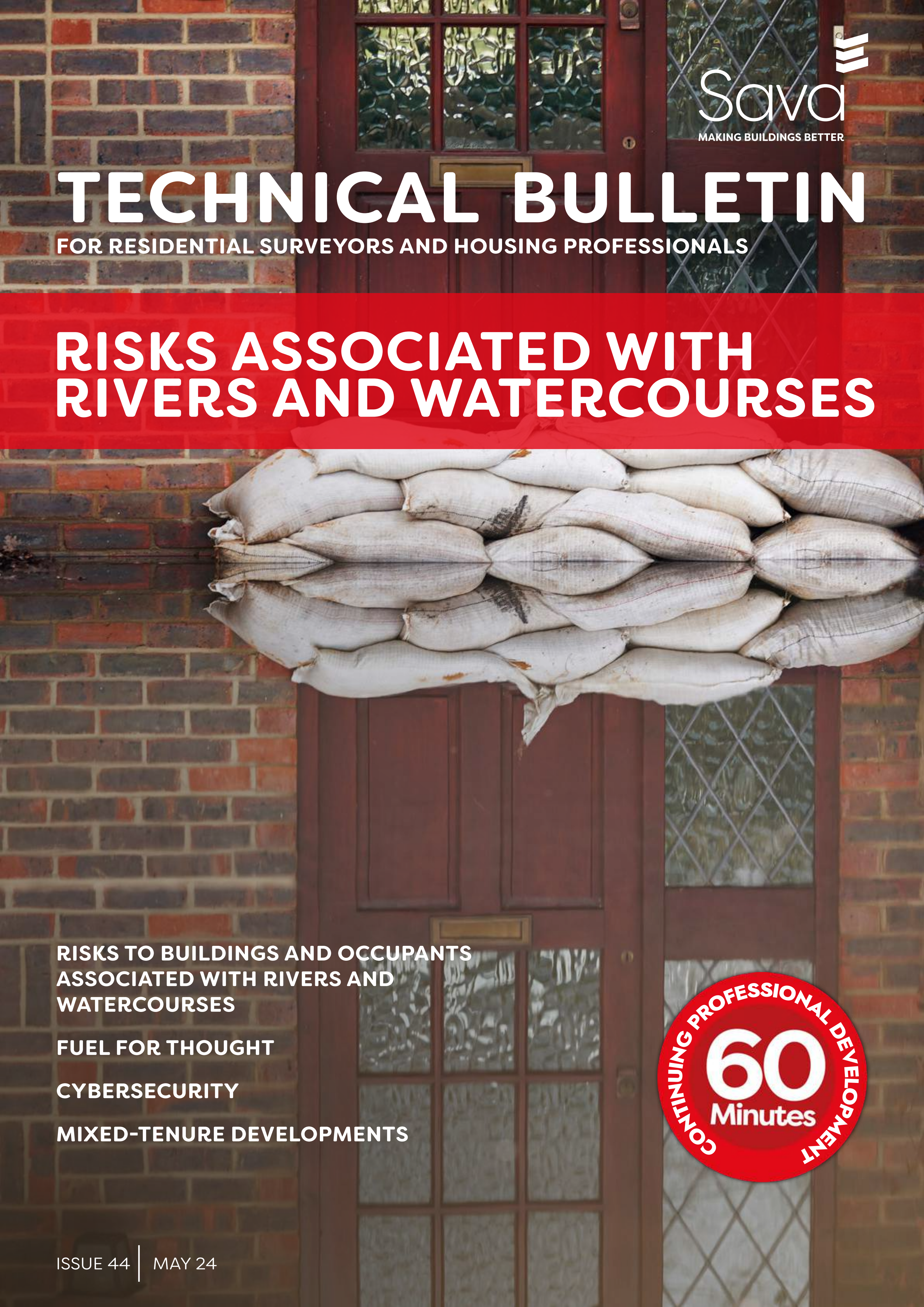


Sava
MAKING BUILDINGS BETTER

TECHNICAL BULLETIN

FOR RESIDENTIAL SURVEYORS AND HOUSING PROFESSIONALS

RISKS ASSOCIATED WITH RIVERS AND WATERCOURSES

CONTINUING PROFESSIONAL DEVELOPMENT
60
Minutes

ISSUE 44 | MAY 24

THE TECHNICAL BULLETIN

FOR RESIDENTIAL SURVEYORS AND HOUSING PROFESSIONALS

Welcome to the Technical Bulletin. This Technical Bulletin is designed for professionals working across all housing sectors.

Produced by Sava, you will find technical articles, regulation updates and interpretation, and best practice. We hope you find this useful in your day-to-day work and we welcome any feedback you may have and suggestions for future publications.

Who we are

We are a team of building physicists and engineers, statisticians, software developers, residential surveyors, gas engineers and business management specialists.

CONTACT

Head office

4 Mill Square Featherstone Road,
Wolverton Mill,
Milton Keynes,
MK12 5ZD

☎ 01908 672787

✉ bulletins@sava.co.uk

🌐 www.sava.co.uk
https://sava.co.uk/sava-edge/

MAKING BUILDIN

CONTENTS

CYBERSECURITY

REDUCING RISK IN A BUSINESS AND KEEPING SYSTEMS SECURE

MATT NALLY, CEO, SURVEY BOOKER

Whether you are a sole trader or a large enterprise, it's beneficial to make your systems more secure than the average firm so that malicious actors move onto lower-hanging fruit. Drawing from his firsthand experience in implementing cybersecurity measures within his own business, Matt Nally, CEO of Survey Booker, offers invaluable insights to help you achieve quick wins in enhancing your cybersecurity.

Cybersecurity is an easy topic to ignore. Most think "it won't happen to me" or "I'm just a sole trader", but even if you're small, you're not unknown. From our podcast on cybersecurity, you'll know that robotic scanners quickly pick up on everything online and you'll be somewhere in a hacking funnel.

If you aren't implementing some basic security practices, you risk being the low-hanging fruit for the sake of a few minutes' effort. It's surprisingly easy to be more secure than the average when so many ignore easy solutions to protect themselves. If you're thinking of moving on to another article, you're either following the steps below or the low-hanging fruit.

What are the key risks to your business?

There are two key risks to your business: people and systems.

Protecting your systems

In today's interconnected world, the risk of cyber threats poses a significant challenge for businesses, regardless of their scale. From data breaches to ransomware attacks, the potential consequences of inadequate cybersecurity can be detrimental to a company's reputation, financial stability, and overall operations. To protect your business from these risks, it is crucial to implement robust cybersecurity practices.

That doesn't mean going back to pen and paper, storing paper files and sending letters by carrier pigeon! Hard copy records have their own risks of being lost, damaged or destroyed. We simply need to look at how you can protect yourself.

For optimal benefits to your business, consider which systems you use that would have the greatest impact on your day-to-day operations and reputation if they went down. For example, if someone was able to hack into your emails, they could:

- send emails pretending to be you
- make payment requests to customers that appear legitimate
- reset passwords for your other systems and gain access

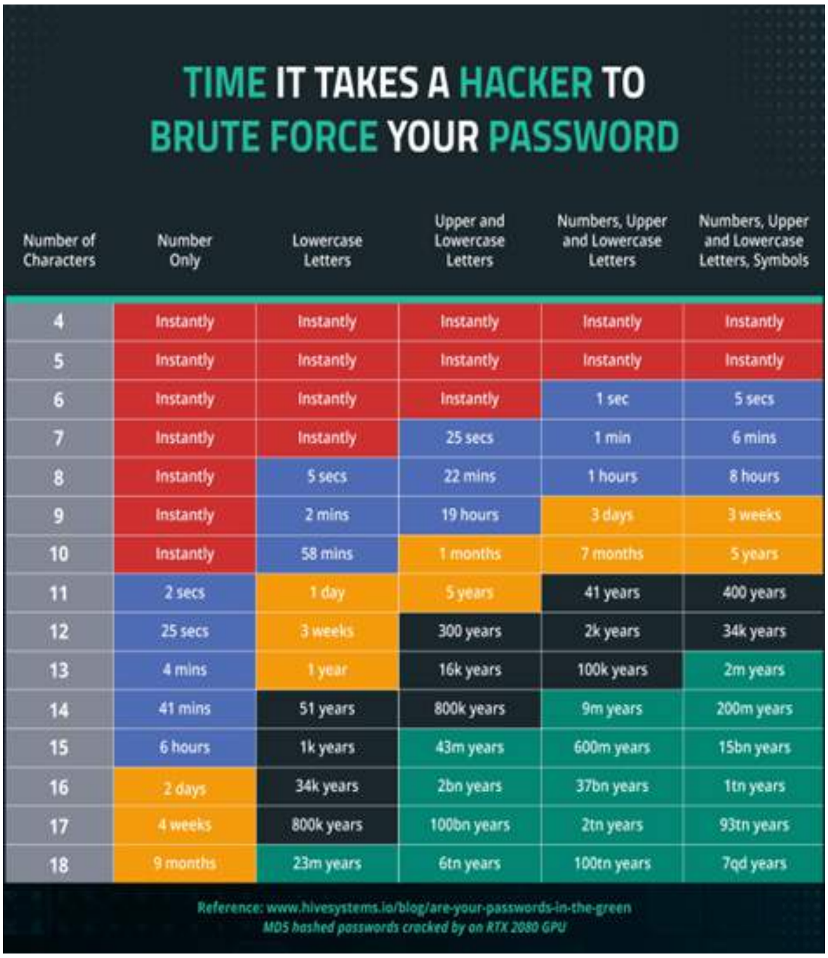
Hence, prioritising maximum security measures for your email system is paramount. Your CRM would be the same as it's central to running your business efficiently. Whereas software for designing marketing imagery or logos may be less of a concern.

So, how can you protect your online systems easily?

Implement a strong password policy

Strong passwords are key as your first step of defence. The golden rules:

- Use a secure password containing letters, numbers, and special characters.
- Don't share passwords—each user must have their own login.
- Don't reuse passwords—if one password is in a data breach, all your systems are at risk
- Don't use similar passwords—one small tweak is easy to brute-force attack (where hackers try lots of similar variations automatically)
- Don't force periodic password resets. This might seem counterintuitive, but the National Cyber Security Centre's advice is not to regularly force password changes. You are more likely to set a weaker password, so you remember what it was changed to. You should change passwords if you think it has been breached.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Number Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hours	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 months	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Reference: www.hivesystems.io/blog/are-your-passwords-in-the-green
MD5 hashed passwords cracked by on RTX 2080 GPU

*Quick tip:
Passwords in the green would be hard to remember and type in each time! Implement a password manager such as LastPass or 1Password. These often have a free tier for individuals. These will generate complex passwords, store them securely and prefill them into login pages so you don't need to remember them!

Does it make that much difference? Here is a graph of how quickly different passwords can be guessed in a brute-force attack (guessed at speed by a computer). Your password complexity takes you from an easy instant hack to virtually impossible.

Lost your device? You can login on another device to your password manager to revoke access to the lost device.

Implement Multi-Factor Authentication (MFA)

It might take 7qd years to brute-force your password. However, passwords alone are no longer sufficient to protect your business from unauthorised access. If someone can guess it or find it in breached data, they are straight into your account and off they go.

Implementing multi-factor authentication (MFA) adds an extra layer of security by requiring you or your team to provide additional authentication, such as a fingerprint, a unique code, or a token, in addition to the password. That way, after your password is entered, you still have one step to go.

MFA significantly reduces the risk of your account becoming compromised even if passwords are stolen or cracked. Survey Booker helps protect you by requiring a minimum complexity of password and offers the option of 2FA and Single Sign On.

Practice regular software updates and patch management

Yes, we've all heard it before. And yes, we all like to keep pressing 'snooze' or 'try again tomorrow' on that update button because we're in the middle of something. However, outdated software often contains known vulnerabilities that cybercriminals can exploit.

To minimise this risk, establish a regular update and patch management process. Keep your operating systems and applications up to date with the latest security patches provided by vendors. Enable automatic updates wherever possible, and regularly check for updates manually if automatic updates are not available.

Regularly back up and protect data

Data loss can be devastating for a business, revealing what you are doing, when and who for. If your data is subject to a ransomware attack or simply all gets deleted, backups ensure that you can easily restore and restart. Of course, that's only helpful if you back up your data frequently, otherwise, you'll still be missing a lot of information.

Again, it's easily ignored but a nightmare when you need to recover your information and you've neglected it. Days and weeks go by very quickly without you realising you've not made any manual backups!

Emails and file storage can easily be set to automatically backup using different systems online, so you don't have to remember to do it yourself. Systems like Survey Booker also regularly back up data for you.

Use a VPN when using public Wi-Fi

As a surveyor frequently on the move, utilising a VPN (Virtual Private Network) is essential when accessing public Wi-Fi networks. While you're likely to stop at places like coffee shops, the majority of public Wi-Fi hotspots are vulnerable to security breaches. This exposes you and your data to potential risks, as malicious entities can easily intercept your device's activities on these networks.

A VPN enables you to encrypt traffic to and from your device and reduce the risk of a malicious actor monitoring what you are doing. This means you can still use public networks but without taking as much of a risk.

Choose your suppliers wisely

Your suppliers not only deliver services to you but also handle your sensitive data. Hence, the security credentials of your suppliers carry significant weight, indicating their commitment to safeguarding your data. Engaging external auditors to assess their practices underscores their dedication to maintaining robust security measures. Suppliers lacking accreditations may overlook vulnerabilities in their systems or processes, potentially exposing your data to risks.

What should you look for? An internationally recognised accreditation is ISO 27001. It's a rigorous process that looks at all aspects of a business's security, from software to people.

Why does this matter? Cyber security is one of the hottest topics at the moment. If a key supplier to your business cannot operate due to a cyber-attack, you can't either, so you want to know they're doing everything they can to keep you running smoothly.

External certifications help you ensure suppliers are meeting specific standards as they undergo audits by accredited third parties. This means you can choose suppliers with your due diligence done for you. For this reason, Survey Booker maintains ISO 27001 certification and undergoes multiple audits each year.

People

While you may have fortified your systems, the most significant risk to their integrity remains you and your team. After all, we're all susceptible to human error. Instances such as falling prey to phishing scams, taking shortcuts, or setting weak passwords for convenience are common pitfalls. So, how can you ensure the security of both yourself and your team?

Educate and train employees on cybersecurity best practices

Provide regular and comprehensive cybersecurity training programs that encompass a wide range of topics, from best practices to recognising common threats and effectively responding to security incidents. Ensure the training is interactive and engaging, using real-life examples and case studies to reinforce the importance of security practices. This makes it easier to spot a suspicious-looking email or form. Additionally, always provide explanations for the rationale behind security measures, as understanding the "why" is pivotal in fostering behavioural change.

Clear Security Policies and Guidelines

Develop clear and concise security policies and guidelines that outline expectations and responsibilities for employees regarding information security. This should cover everything from password policies, clear desk policies and leaving devices unattended.

Phishing simulations and testing

Phishing is when 'attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware or direct them to a dodgy website' (National Cyber Security Centre).

How do you test if your team can spot a malicious email or text? Regularly conduct phishing simulations and testing exercises to assess employees' susceptibility. These are where employees see an email and fall victim to not realising that it is a malicious email designed to harvest credentials. These simulated attacks can help identify areas where additional training or awareness is needed so they don't fall victim to a real one.

Restrict what your team has access to

Team members should only have access to data they require. Regularly review and update access permissions, particularly during role changes or when employees leave the organisation. This proactive approach serves to prevent an employee from maliciously making changes or deleting data as many attacks can start from within. Moreover, it safeguards your business in the event of compromised accounts, as hackers face limitations in making system changes with reduced access levels.

Mobile device management

It happens more often than we'd like to admit – people misplace or lose their devices all the time. Whether you've accidentally left your tablet on the roof of your car, or your phone has fallen out of your pocket on a train, these incidents are commonplace. A mobile device manager allows you to connect your company devices to the device manager and you can remotely lock or wipe a lost device so that any data contained on it can't be accessed by a third party. The risk of losing a device is also why you should store all your data on the cloud and not on the device itself!

Conclusion

Protecting your business from cyber threats requires some planning. While it may be tempting to overlook this aspect and hope for the best, implementing quick and effective measures now can significantly bolster your security. Investing just a couple of hours now could potentially save you hours of headache in the event of a data breach.

What are the easy wins you can implement after reading this article:

- Implement a password manager and strong password policy
- Implement multi-factor authentication
- Check if the certifications of suppliers you are using and consider moving to accredited suppliers

Want to learn more about mitigating business risks?

Check out our podcast where we have episodes with cybersecurity specialists, ISO 27001 auditors and more. They share their insights on how you can best protect your business and help keep yourself safe and secure.

About Survey Booker

Survey Booker is the industry's leading CRM and Survey Management System. Whether you are looking to reduce the amount of time lost on admin, grow sales, collaborate better as a team, ensure all your compliance is handled, provide a better experience to customers or increase profitability, our customisable system adapts to your needs. Contact Survey Booker to find out more www.surveybooker.co.uk

ONLINE TRAINING MODULES

Enhance your housing knowledge with our fully online training modules, designed to help you learn where you want, when you want.

Courses available covering:

- Invasive non-native plant species
- Walls, floors and roofs
- Inspection technique
- Damp and condensation

...and many more.

Scan to browse our courses

www.sava.co.uk/qualifications

Sava

Sava
MAKING BUILDINGS BETTER