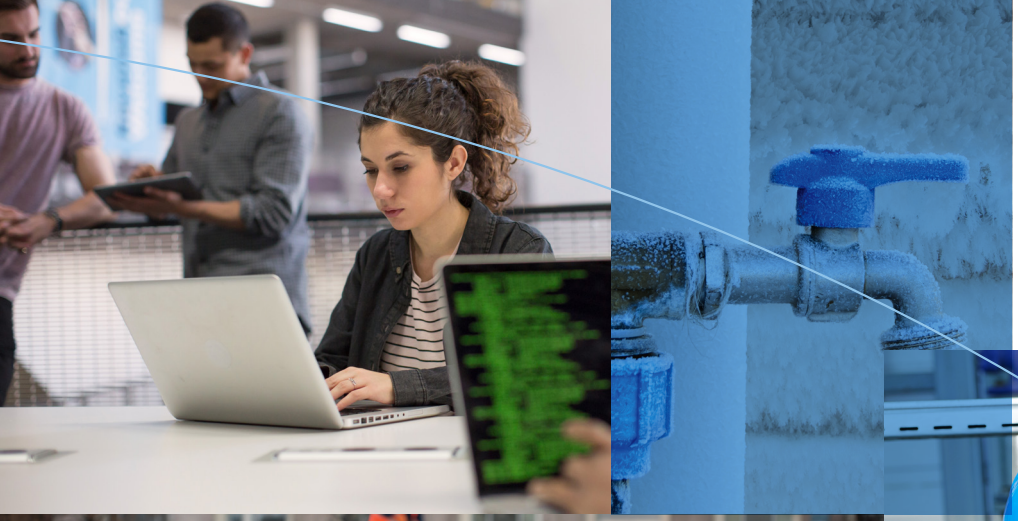


Gallagher

Insurance | Risk Management | Consulting

COMMUNITY MATTERS

WINTER 2022

INTRODUCTION

Welcome to the latest issue of our Community Matters newsletter featuring topical articles for the Community sector, including local councils, charities and not-for-profit organisations.

With the cold season approaching it is essential to be prepared to protect your buildings, so in preparation of what approaches, take a look at our guidance on protecting your buildings during the winter.

In addition to this, we've prepared some advice and information on cyber tips for local councils and communities.

You'll find regular updates and helpful information from the underinsurance of community buildings to insurance considerations for events and much more in our news and insights section of our website.

We'd love to hear any suggestions for future articles—please send us your suggestions via email us at uk.community@ajg.com.

Connect with us

Our Gallagher UK **LinkedIn** and **Twitter** channels are also a great way to stay up to date with the latest news and insights so please follow us.

COUNCILS AND COMMUNITIES— PROTECTING YOUR BUILDINGS DURING WINTER

Taking care of buildings and structures throughout the winter months can be vital for councils, charities and community groups, not just from a cost perspective but also for the health and safety of the people they serve.

Council and community buildings are so much more than property assets for the organisations that own and manage them. They can be essential for the communities who rely on the services provided from these spaces as well as those who work within them.

Preventative and planned maintenance can help you protect your buildings during cold snaps and inclement weather to keep your services running smoothly and reduce the risk of expensive repairs or liability claims.

External building maintenance

Taking a top-down approach, examine the roof for signs of damage, missing tiles, etc. Do this before the winter weather sets in and potentially makes the job more hazardous. Damage in a neglected roof can quickly become worse in stormy conditions or heavy snow/rain, with problems extending to the inside of the building. This could go on to cause issues such as structural damage internally, potentially leading to a period of business interruption while repairs are carried out, as well as the cost of the repair.

Drainage channels, such as downpipes and gutters, should be clear of debris to avoid blockages. Doors and windows should be inspected for gaps and, if necessary, fixed with caulk or weather-stripping material to reduce the escape of heat.

Internal building maintenance

It is important to keep your buildings running efficiently during the colder weather while you are increasing your usage of heating and lighting.

Add extra insulation to the roof if possible, and ensure water tanks, pipes and radiators are adequately lagged.

If pipes freeze, isolate the pipe by closing the stopcock on the feed, then protect items beneath it before thawing the pipe. To thaw the pipe, apply heat slowly using a hair dryer, space heater or electronic heating pad—do not use hot air paint strippers, blow torches or naked flames.

Trees near buildings

Any trees close to your buildings should be inspected by a qualified arborist to ensure they are structurally safe. If necessary, trees should be pruned or removed to avoid damage to external structures caused by falling branches or the entire tree. Not only is this important to avoid damage to your buildings, but to meet your health and safety obligations to the public and your employees, and reduce the likelihood of liability claims in the event of injury.

Clearing snow and ice

The Workplace (Health, Safety and Welfare) Regulations 1992 and the Highways Act 1980 state that arrangements should be made to minimise risks from snow and ice on roads and paths.

To help ensure safe access to your buildings during snowy weather, prepare items such as snow shovels, grit and de-icers, and make sure they are easily accessible so that heavy snowfall incidents can be dealt with quickly. Monitor weather alerts and grit the pathways the night before snow or ice is expected, if possible.

While it is not the case that liability for injury lies with your organisation if snow and ice are cleared and somebody still slips and falls, it is important to ensure that clearance procedures do not create more of a hazard. For example, the use of water to melt snow or ice can create 'black ice' that can be difficult to see, so you should use grit, sand or even ash to provide grip underfoot. Inside the building, you should have adequate 'wet floor' signage at the entrance, and plans in place to regularly mop/dry potentially hazardous areas.

Flood protection and damage limitation

While it is possible, to some extent, to protect your buildings in the event of flooding in adverse weather conditions (through physical solutions such as sand bags, drain non-return valves, air brick covers, etc.), it is also important to have adequate levels of flood cover in place. We can support you by arranging this, even if you have had difficulties securing this kind of cover in the past. We will base your cover on your actual exposure to flood and calculate an estimated maximum loss, and we can also offer flood excess insurance to cover the flood excess amount.

In addition to providing flood insurance cover, Gallagher provides a risk management service which includes flood inspection, reporting and surveys. We can act as your risk management partner to help you build a flood contingency plan to reduce your exposure but also speed up recovery should your premises suffer flood damage.

SNOW AND ICE

We recommend councils should consider the following:

1. A written risk assessment should be carried out and kept on council's files.
2. The council should take reasonable care to ensure the safety of the public, employees and volunteers.
3. All employees and volunteers should be made aware that the clearance of snow and ice could be a seven-days-a-week task (including bank holidays), receive adequate training, and wear the appropriate protective clothing.
4. We recommend that the council communicates its plans to the community. This can be via a website, newsletter, noticeboard or published minutes of a meeting. If a plan changes, this should also be communicated effectively.
5. Once a clearance programme is implemented, it should be maintained for the whole period of adverse weather and the plans on how the process will be managed should be communicated.
6. Where a council takes on the responsibility for clearing snow or ice from paths, it should exercise reasonable care in doing so. Care should be taken in deciding where to move the snow—make sure entrances, side roads or drains are not blocked. Clear the middle of the path first so there is a safe surface to walk.
7. After the snow and ice has been cleared, do not use water as this may cause black ice. Use salt or grit to treat the areas.
8. Also, if the building is to be used over the winter, the council needs to ensure that 'users' can enter and leave the building safely, which means that if they are not gritting the paths or car park then the building should be closed for that period.

GUIDING THE CYBER CONVERSATION — TIPS FOR LOCAL COUNCILS AND COMMUNITY GROUPS

Typically, public sector and third-sector organisations have been slower than other sectors to invest in their cybersecurity. This may be due to underestimating the risks, overestimating the costs, or a mixture of both.

For many local councils and community organisations, while there is recognition of the need for assistance with their cybersecurity obligations, a lack of understanding of the complex digital landscape can prevent or delay positive action.

"Where do we start?" and "How much will this cost?" are valid questions, not least because the cyber landscape changes almost daily. With the numerous responsibilities, budgetary challenges and time constraints that your organisation faces, it's no wonder cybersecurity can seem like an overwhelming topic for smaller organisations.

So, how can you strengthen your digital armour and reduce the likelihood of liability claims, business interruption or reputational damage caused by a cyber incident?

Let's break it down...

It starts with the Board

Cybersecurity is central to an organisation's resilience, and this places it within the responsibility of the board. While technical expertise is not expected, board members need to have a level of understanding that is sufficient to ask the necessary questions and have fluid conversations with the relevant experts.

This will help you identify your organisation's vulnerabilities, who might target you and why, and how they would do it. You can then begin to work with your cyber specialist on the integration of your cybersecurity plan into your operational risk management processes.

Employee training is key

The biggest cyber risk faced by organisations is not from cybercriminals but from complacency and human error within the organisation itself. Therefore, it is important to develop a positive cybersecurity culture, with the board instilling a commitment to cybersecurity awareness throughout the organisation. Training sessions can cover a host of topics, from common cyber-attacks such as phishing and ransomware to the common security risks associated with home working and BYOD (Bring Your Own Device) scenarios.

Seek the expertise of cyber security specialists

Having a cyber specialist work alongside you to manage your cyber risk can prove vital. They will have the tools and expertise to help you strengthen your organisation's defences, and have their finger on the pulse when it comes to new and evolving threats.

Some of the services available can include:

Cybersecurity awareness courses: Helping your organisation identify and avoid the most common pitfalls, and supplying Cyber Essentials' compliance and accreditation services.

GDPR audits: Identifying practices and processes that fall outside of compliance with the General Data Protection Regulation and recommendations for the actions required to achieve regulatory compliance.

Phishing simulation exercises: Users will be targeted and encouraged to click on links or open attachments in an email to identify what percentage of a workforce is cybersecurity aware and what percentage is vulnerable following a social engineering attack.

Penetration testing: An ethical hack of your network to identify vulnerabilities, both externally and internally. This can be an eye-opening experience!

Vulnerability scanning: Ongoing vulnerability scanning against your publicly-facing assets, identifying potential vulnerabilities and the steps to remediation.

Developing an incident response plan

While prevention is better than cure, it is not possible to prevent every cyber-attack or data breach. It is therefore essential that you know what to do when this happens.

You must report a data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it. By definition, this is a breach of security leading to "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

This does not apply if you can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of the individual(s) involved.

Your responsibilities, however, do not end there. Having a robust incident response plan in place can help your organisation to recover from the incident financially, and from a reputational and business interruption perspective.

A cyber risk management specialist can prove their worth after the event by quickly capturing and analysing information, eradicating the threat/lowering the impact, and recovering data and systems.

If you would like to speak to us about your organisation's cybersecurity, please get in touch. We can provide the relevant cyber liability insurance and also support you from a risk management perspective through all of the specialist services mentioned above.

UK COUNCILS HIT BY 10,000 CYBER-ATTACKS EVERY DAY SO FAR IN 2022

Cybercriminals are increasingly targeting UK councils,[1] with more than 2 million attempted cyber-attacks recorded in 2022 to date.[2]

There has been a
14% rise
in the number of cyber-attacks year-on-year.[3]

Phishing attacks are the biggest threat to councils
with 75%
stating it is the most common type of cyber-attack experienced.

A Freedom of Information (FOI) request from insurance broking and risk management firm Gallagher investigated the scale of cyber-crime against UK councils, with 161 local authorities sharing information. Based on the proportion of councils who shared data on cyber-attacks, the size of the problem is likely to be significantly greater. Scaling up these figures accordingly to reflect response rates, the true number of attacks across all councils is estimated to be more than 11 million in 2022.[4]

While most cyber-attacks are intercepted by IT security put in place by local authorities, the councils who shared data revealed that they had paid out over £10 million over the past five years due to cyber-crime. This includes monies lost to hackers, legal costs and fines.

Phishing attacks are by far the biggest cyber threat to councils, with three-quarters (75%) stating that it was the most common type of attack that had been attempted against them.

Distributed denial-of-service (DDoS) attacks, which attempts to disrupt web traffic or services by overwhelming servers, were the second most common attempt type—ranking as the top threat this year for 6% of councils.

The increased prevalence of cybercrime has been exacerbated by increasing digitisation driven by the pandemic—affecting both the public and private sectors. In fact according Gallagher statistics, 15% of UK business owners say cybercrime is one of their biggest risks, specifically driven by the increased reliance on technology post-pandemic.[5]

As a result of this growing risk, in the last 12 months around half of councils (52%) have needed to employ an external expert to give them advice on how to mitigate the risk of cyber-attacks.

Nearly nine in 10 councils (85%) have increased their cybersecurity to help them cope with the volume and sophistication of attempted attacks, but despite these increased efforts to help guard against the growing threat, currently only 23% of councils currently hold a cyber-insurance policy to protect against the potential consequences.

[1]Based on Freedom of Information requests sent to 426 councils across the UK on 20 June 2022. Of these, 243 responded before 15 August 2022, with 83 councils refusing to share the data, either due to exemptions or it not being held, meaning 160 councils shared at least some of the data requested.
[2]2,274,188 attempted cyber-attacks in 2022 were reported by UK councils. 88 councils responded with data as a result of this section of the Freedom of Information request.
[3]2,274,188 attempted cyber-attacks in 2022 were reported by UK councils. This is 14% more than the 1,996,204 attempted cyber-attacks reported by UK councils in 2021 in the same FOI request.
[4]With 88 councils providing specific data on the number of attempted cyber-attacks experienced in 2022 from a potential 426, this indicates that as many as 4.8 times many more cyber-attacks could have been attempted in 2022. With 2,274,188 having been reported, this indicates as many as 11,009,137 could have actually taken place—which is rounded down to 11m as an estimate.
[5]Additional data from Gallagher research conducted by 3Gem, between 8 May and 16 May 2022, among 1,000 senior decision makers in UK businesses.

Commenting on the findings, **Johnty Mongan, Head of Cyber Risk Management at Gallagher**, said: "Criminals unfortunately only know too well that cyber-attacks can cripple systems and with many councils increasingly servicing local people's needs digitally, they simply cannot afford to experience downtime. It is positive to see that councils are recognising this threat, and looking to employ external experts to help prevent cyber-attacks—risk management and putting in the right security is absolutely key and external experts are best placed to advise what the most up to measures are."

Tim Devine, Managing Director for Government, Housing, Education & Public Sector at Gallagher, said: "It is important to have a plan in place should the worst happen. With so many attacks happening every day, it only takes one error to cause significant problems. The risk in terms of associated costs and reputational damage as a result of cyber threats means having specialist cyber insurance in place should be a key consideration but is by no means the only consideration for those wishing to mitigate the risks of an attack."

Connect with us

To find out more, please contact us.

T: +44 (0)800 062 2030 | E: community@ajg.com

Gallagher

Insurance | Risk Management | Consulting