RISK INSIGHTS

BLACKFRIARS GROUP INSURANCE

Cyber-security for Local Councils

As a leader within your community's local council, you possess the unique and fulfilling responsibility of ensuring local communities are healthy, safe and successful. However, such a profession comes with serious risks. Indeed, providing a wide range of public and organisational services to your community requires safe handling, processing and storage of various data—including that of local communities' sensitive records (eg financial, health-related or contact information).

In the era of evolving technology and strict data protection regulations under the GDPR, a data breach within your local council could lead to costly consequences. And recent research from iGov and Freedom of Information Requests revealed these instances are far too common—more than 75 per cent of UK local authorities experienced some type of cyber-attack in the past five years, while more than 25 per cent of UK local authorities experienced an actual cyber-breach (meaning criminals successfully breached their systems).

The same research found that Britain's local governments were hit by 98 million cyber-attacks over the past five years. That equates to 37 attacks every minute. Your local council simply can't afford to ignore the risks of lost or stolen data, costly non-compliance fines and reputational downfall that accompany a cyber-attack. Review the following cyber-security best practices and data breach case studies to ensure proper protection against a cyber-incident.

General Cyber-security Best Practices

The key to establishing proper cyber-security within your local council is to make cyber-risk a priority throughout your organisation—starting with the leaders on the board. When conducting your routine risk assessment, be sure to address cyber-risk.

Your local council simply can't afford to ignore the risks that accompany a cyber-attack. Consider these best practices to protect against a breach.

From there, it's important to create supporting risk management policies and introduce effective cyber-security controls within your council. For example, implement these best practices:

- **Maintain network security** by ensuring a safe and secure internet connection on workplace devices, installing proper antivirus and malware protection, scanning all media for malicious content before importing it and performing software updates.
- **Manage employee privileges** by limiting the amount of users with access to sensitive data and monitoring their activity. Require employees to regularly update passwords and save sensitive information in appropriate locations. Routinely train staff members on proper cyber-security practices, such as how to detect phishing and safe device use. Use practices such as encryption to further protect data during a breach.
- **Establish a cyber-incident response plan** that allows for a smooth, efficient and speedy recovery in the event of a breach. The response plan should address a variety of potential cyber-scenarios, be compliant with relevant regulations and be tested

regularly for effectiveness. Communicate and practise this plan with all staff members.

- **Enforce cyber-risk management policies** to all staff members. This should include a safe internet and email use policy, BYOD policy, mobile working policy and data breach response policy.
- **Monitor cyber-security practices and controls** for effectiveness. Make changes and updates (and communicate them to staff) as needed.

GDPR Compliance

Following GDPR standards is crucial to ensure effective data protection practices and avoid hefty non-compliance fines. Consider this guidance:

- Make sure all staff members fully understand what the GDPR is and how they play a role in helping your local council remain compliant. This includes:
    - Knowing what a personal data breach is and how to properly identify it
    - Being aware of the local council's data breach response plan and knowing how to escalate a potential breach to the correct person or team (this includes reporting a breach to the ICO within 72 hours of detecting it if the breach is likely to result in a risk to people's rights and freedoms)
    - Understanding the amount of cyber-risk the local council faces and engaging in routine data protection/GDPR training to properly perform risk management controls
- Review your existing data processing practices to ensure that your local council identifies with one of the six lawful bases for processing.
- Depending on your position in local government, you may be subject to a data protection fee. Click here to determine if payment is necessary.
- Review your existing data sharing agreements and be sure they comply with GDPR standards. For any new or revised agreements, conduct a data protection impact assessment.
- Properly document all data processing and storage practices. Click here for information on documentation standards.
- For more information and guidance on GDPR compliance, click here.

Social Media Risk Management

As social media becomes increasingly popular, it's important for your local council to maintain an online presence. However, be sure to only allow competent employees to run your local council's social media accounts and have access to the passwords. In addition, consider these tips:

- Be responsible and respectful during all social media interactions. Ensure your posts follow local council HR policies.
- Only share content and links from reliable sources. Always provide credit.
- Establish a routine posting schedule. Make sure content engages your audience by asking questions and offering feedback to comments.
- Be honest at all times. Don't try to cover up mistakes. Use social media as an opportunity to be transparent with your community.

Local Council Case Study: A Good Example

In 2017, the Copeland Borough local council suffered a serious cyber-attack. The council had no access to shared or personal drives and was unable to use key operational systems (eg payroll services and electronic election software) for an extended period.

Although the attack was unavoidable due to the hacker using unrecognisable hacking software, the council responded to the incident efficiently by implementing their business continuity plan, assembling a specialist IT team, meeting with staff members to update them on the situation and informing the proper authorities. Moving forward, emergency resources are now stored

in web-based backup locations to ensure continued operational success during a breach, and staff has undergone further cyber-security training.

Despite their efficient response, the attack still cost the council £2 million in restoration efforts, new equipment, employee training and more.

Local Council Case Studies: Bad Examples

- In May 2017, a council in the East of England was fined £150,000 for publishing personal family information in planning application documents, which it accidentally made publicly available online.
- In October 2012, a West Midlands council was fined £120,000 for accidentally disclosing personal data via email to the wrong recipient.
- In May 2017, a South West council was fined £100,000 for leaving personal information vulnerable to cyber-attacks.
- In August 2016, a South East council was fined £100,000 because its data controller failed to take appropriate organisational measures against the unauthorised processing of personal data.

This is just a small selection of recent, large fines levied against local councils for cyber-related breaches. Whether the cause was a targeted cyber-attack or an employee mistake, most cyber-breaches can be stopped with both robust cyber-security and mandatory employee training.

The Need for Employee Training

An element of human error is responsible for about 80 per cent of all cyber-breaches, according to ICO data. That means that some human intervention is necessary for the breach to be successful, whether that involves an employee mistakenly responding to a phishing email, clicking on a link containing a virus or sending a sensitive email to the wrong recipient.

Despite holding sensitive data, the widespread human error and the stiff financial penalties, 75 per cent of local councils do not provide mandatory employee cyber-security training, and 16 per cent provide none at all. Staff training is vital to protect against one of the most common cyber-exposures: your employees. Click here for government guidance on staff cyber-training, and ask us for copies of our Employee Cyber Training Manuals.

Ask These Questions to Gauge Your Readiness

To start assessing your local council's cyber-security, ask yourself and other council leadership the following questions:

- Is leadership aware of our unique cyber exposures?
- Is cyber-security part of our continuity plans?
- What data and information standards and protocols are in place?
- What kind of processes and tools do we have in place to prevent cyber-attacks?
- Is appropriate and proportionate training provided to all staff, including scenario exercises?
- What reporting mechanisms are in place for staff to report cyber-security concerns?
- Do we have the technical capabilities to manage an attack? Is this tested regularly?
- What is our communications plan in the event of an attack?

Purchase Robust Cover

More than anything, you can ensure ultimate peace of mind against a cyber-attack by purchasing robust cyber-insurance. For more information, contact Blackfriars Insurance Brokers Ltd today.