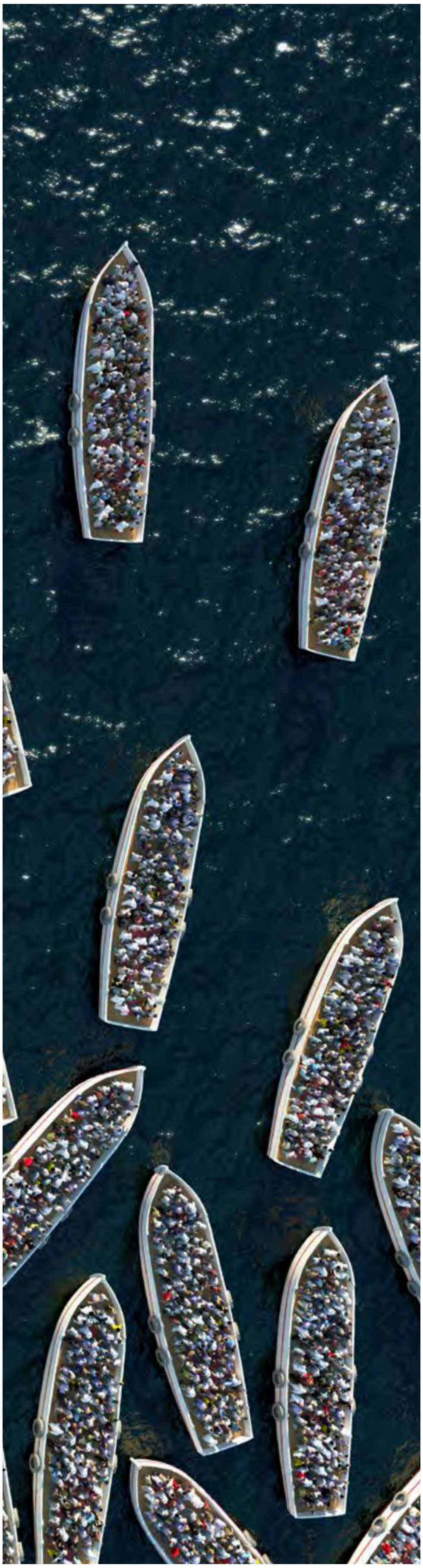
Understanding the Cyber Challenge for Membership Organisations

EQUANTIIS

Contents

Introduction



There are over 8,000 membership organisations and associations based in the United Kingdom. Whilst the sectors, number of members, available resources and services differ, they all have one thing in common. The threat of disruption to business and knock on effects following a cyber-attack.

There are limited cyber security statistics available for the membership sector - the most comparable sector would be 'charities'. In 2018, two in ten charities experienced a cyber security breach compared with four in ten businesses.

As more and more membership organisations transfer services and data online, the risk of more breaches is certain and the myth of being too small to be a target will be expelled.

There are some challenges to achieving effective cyber security management in membership organisations, for example:

- **Tactical not strategic view**
- **Lack of enabling culture**
- **Limited supporting governance structures**
- **An inadequate security regime**
- **Resource constraints**

It starts with strategy

Cyber security is not a project. It will not be completed. So, it requires strategic thinking, and that thinking needs to be constantly challenged and periodically reassessed.

The starting point is to consider what the target actually is: What are the organisation's crown jewels? For a membership organisation this would typically be a combination of the following:

1. Customer Data

2. Money

3. Intellectual Property

4. Brand Reputation

Once this is ascertained, a review can be undertaken to understand the risk and what is required to protect these assets.

It is also critical to understand what regulatory responsibilities need to be met when it comes to data protection and security. The obvious being:

- The General Data Protection Act (GDPR)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR)

If a membership organisation also has charity status or fundraises then there may be additional checks and balances with the Charity Commission, Fundraising Regulator or Gambling Commission. Additionally, if they provide insurance to members, then they would also need to adhere to the Financial Conduct Authority (FCA) principles, in particular Principle 11 which states that you must report a material cyber incident.

It is also important to accept that cyber security is not just an IT problem and is actually an organisation wide challenge.

Don’t underestimate the impact of culture

To successfully see off cyber threat and protect data requires an enabling culture. Cyber security is often seen as a low priority within the senior management teams of membership organisations, as compared to other sectors.

A common rationale is that they are unlikely to be a target of cyber-crime because they are too small; not in the same league as government bodies or big corporates; or don’t process particularly useful or sensitive data. This denial of risk, compounded by typically slow-moving decision-making processes, lack of resource and ownership, leaves membership bodies exposed.

People remain a key target for criminals and not every attack is committed via hacking a computer server system. Many attacks are committed via a simple communication via email, on the telephone and face-to-face as it is always easier to login with a password or get an employee to undertake the action albeit unknown to them.

Phishing emails are still a big threat to organisations. These emails are getting harder to spot due to an improvement in the quality of language used and the introduction of targeted content, such as the name of a CEO or Finance Director, as a result of our increased social footprint. According to UK Finance, CEO fraud was responsible for a total loss of £148 million in 2018.

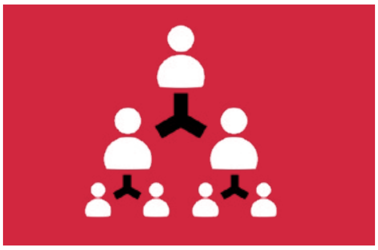
It is also important to ensure there are processes in place to restrict uninvited face-to-face visitors to buildings, as they can physically connect to a network or install key loggers to intercept information, or find passwords which are scribbled on Post-it notes.

An enabling culture

In relation to cyber security and data privacy, an enabling culture means:

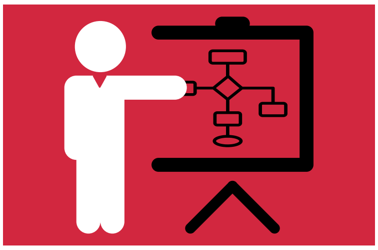
It must be high on the agenda, owned and and pushed by senior management.

Having the agility to be capable of rapid response to identified threats – streamline the decision-making process.



Everyone taking ownership and doing their part to keep the organisation's assets safe.

Learning from mistakes and taking the opportunity to make improvement, rather than attributing blame.



Education, process and policy is critical to ensure that staff are aware of the risks, and also, their responsibilities.

The governance equilibrium

Membership bodies tend to have limited governance structures in place, which can lead to lip-service being paid to risk management and inadequate oversight. Businesses continually change - they have to for survival.

Larger businesses tend to have processes in place to govern third party take on, process or technology change. Membership bodies occasionally have some structure around these areas, but it is generally limited. The lack of change governance can introduce risk because third parties and technologies aren't vetted adequately, or a new process introduces risk.

It's important to not prohibit change, equally light touch governance is necessary to maintain enough control to enable successful cyber security management on an ongoing basis. The recent British Airways investigation by the Information Commissioner's Office is a good illustration of IT governance gone wrong. The vulnerability exploited by hackers was a known one and the BA system had not been updated since 2012 .

Complexity is added by volunteers running local or specialist professional groups, because they typically operate like a third party - using their own infrastructure; remote; not subject to a contract of employment; and with limited time available. These groups typically present major security and data privacy risks due to lack of oversight.

Good governance

Good governance to support data privacy means:

A robust approach to risk management to ensure risks are identified, sized and remedied appropriately.

Keeping up-to-date with both internal and external risks as they change and reacting quickly.

A procedure to ensure an appropriate level of due diligence is conducted on all third-party processors, including cloud service providers, prior to on-boarding.

Basic change control or project approval procedures to identify and risk assess proposed change to policy, process or technology.

Treating volunteers as employees for the purposes of data privacy and security so that they are clear about their contracted responsibilities and your procedures; and adhere to the same level of security as expected of an employee.

The thin grey line between adequate and inadequate

A common question asked by membership organisations is how much is an appropriate amount to invest in cyber security and data protection? There is no binary answer to this and certainly the GDPR talks about measures needing to be 'appropriate' to the organisational context and the perceived risks, rather than specific monetary values.

How can an organisation determine what an 'adequate' security regime looks like? It is vital to take a strategic approach to security so that the organisation's key assets and the risks are identified, assessed and the security regime implemented reflects the identified risk. If an organisation can demonstrate that it has taken this approach, then the assumption has to be that any fine would be lower, as compared to an organisation which is wilfully negligent and does nothing.

Many membership organisations use an outsourced IT service provider and, with limited internal technical expertise, there tends to be an assumption that the third party will have implemented an appropriate level of security. Unless they have been given explicit instruction or have been involved in your risk assessment and the measures required to reduce risk, it is unlikely they will have enough information about your unique circumstances to be able to implement an appropriate security regime.

Outsourced relationships for IT need to function like a partnership, rather than like supplier / customer. There needs to be engagement, discussion and consensus around security and privacy requirements.

The security regime in place should also be audited for adequacy by an independent organisation on a regular basis and working towards Cyber Essentials and other standards like ISO27001 is a good way to get on the right side of that thin grey line.

Where to start with systems

60% of attacks are carried out by insiders

With this in mind it is essential that organisations consider both 'privacy by design', a principal from GDPR, but also 'security by design'.

This becomes an organisational responsibility as systems are now often spread across an organisation and ownership of 'security' is not considered. Whilst security shouldn't be owned by IT, there are lessons that could be shared with other departments.

Websites and email solutions are typically owned by a Marketing Team, who would not necessarily know how to implement a robust patching schedule and accompanying change management process. Even if the website is managed by a 3rd party it's fundamental to ensure critical updates are installed in a timely manner to stop vulnerabilities being exploited.

Access to these systems and social media websites should only be granted to those that need them and where possible accounts should be tied to individuals so that an audit trail can be ascertained if required.

Account access should also be tied to the staff exiting process so that access is terminated when an employee leaves. If they have access to shared passwords, such as a social media account, then this must be changed at the same time. Considering the use of a password management tool can also help in this area.

Deliver everything with nothing

The trouble with cyber security and data privacy is that they are invisible until disaster strikes and the measures put in place are shown to be inadequate. With senior management in membership bodies tending to rate cyber security as low priority, it can be difficult to prove the business case for investment because it's a 'what if' type scenario and they simply do not believe they are a likely target.

Money tends to be spent on other priorities for spending instead, e.g. revenue generating activity like Marketing.

According to a 2018 government survey, membership bodies spent on average just £1,940 on cyber security in the previous financial year.

Additionally, membership bodies often don't merit an official Data Protection Officer under the GDPR and so someone usually draws the short straw and has to juggle two roles. Similarly, smaller membership bodies often do not have a skilled cyber security expert in house, which places them in the hands of someone who lacks the skills or with a third party who may not understand the environment enough to make appropriate provisions.

Securing investment in cyber security is key and may require some creativity. This may be a case of highlighting the risks and the dangers of an inadequate regime, which might include the size of the monetary fine a GDPR breach may result in. Using recent case history like the Marriott and British Airways fines under GDPR may lend weight to your business case.

To conclude

Cyber security presents a significant challenge for membership organisations. Financial resources do play a significant part in this challenge because membership bodies typically do not have the budgets seen in big corporates and securing budget for an invisible threat is notoriously difficult. Even so, a more strategic approach to the threat posed by cyber security would enable available resources to be used more effectively.

Essentially, good cyber security is more a management issue, than a technology one in many respects. A reactive piecemeal approach is ineffective and puts organisations and the data they process at risk. Let's remember that the monetary impact alone of a data breach involving personal data can be as high as 4% of global revenue.

Effective cyber security must begin with understanding internal assets and the external regulatory environment, followed by a risk-based approach to proactive remedial action, some of which will involve enabling technology and appropriate budget to support it. However, it is important not to overlook the importance of people.

The culture needs to be one in which cyber is prioritised from above; everyone recognises and is recognised for playing their role; there is agility to respond quickly; and where learning to support continuous improvement is encouraged. Conducive supporting structures and an effective and regular training programme can make all the difference to an organisation's ability to maintain pace with the ongoing and ever increasing threat presented by cyber crime.

Author

Nick David
Executive Consultant
nick.david@equantiis.com

Contact Equantiis

✉ hello@equantiis.com

@equantiis

020 3376 7447

EQUANTIIS