Arthur J. Gallagher
BUSINESS WITHOUT BARRIERS™

BUSINESS INSURANCE BULLETIN

MARCH 2014

ARE YOU CYBER ASSURED?

Cyber risk is gaining profile within the Charity sector and as our case studies show, not just for the largest organisations. There's more helpful information becoming available on the subject but many Charities still feel ill prepared for the potential threats. So how does your cyber risk management stack up and how can insurance help?

In this bulletin we explain the range of insurance protections available and offer practical advice on how to protect your organisation, review data and procedures and identify weak spots, as well as how to remedy them.

Cyber risk is becoming a bigger risk for Charities, and not just for the largest organisations – as these case studies[1] show

Case Study 1

Southampton and District Group of Diabetes UK became aware that their kind donors had been scammed by criminals hacking the Hampshire Charity's Yahoo email account. Scammers sent an email to over 300 donors requesting new donations were made. The leaders of the small local group were alerted to the problem when worried supporters asked them about the email, and by Yahoo who noticed changes to the account and emailed the group. The scammers had sent out a first email from diabetesuksouthamptongroup@yahoo.co.uk followed by a request for money from a hoax account called diiabetesuksouthamptongroup@yahoo.co.uk.

Could this be insured?

Certainly phishing scams such as that suffered by the local Diabetes UK group can be covered with insurance paying out for the cost of creating and issuing a specific press release or establishing a specific website to advise supporters of the fraudulent communications; the cost of reimbursing existing supporters for any financial loss directly arising from the scam: and any impact to your income resulting from the fraudulent communications. One leading insurer has already confirmed to us that this instance most certainly would have been covered.

Case Study 2

Norwood Ravenswood were fined £70,000 in October 2012 by the Information Commissioners Office (ICO) after information about the care of four young children was left outside the London home of their prospective adoptive parents one evening in December 2011. Whilst the Charity has hit back stating that the fine is "disproportionate" and reserved the right to appeal the ICO are sticking to its guns responding that the incident was "entirely avoidable" and using this as a warning to all Charities to fulfil their obligations under the Data Protection Act.

Could this be insured?

Insurance could have paid for the costs around notifying the breach and contacting those whose information was breached, as well as privacy liability, and where legally permitted as insurable, regulatory actions and investigations including the penalty imposed.

Other examples

In May 2011, following the theft of laptops which included data about children they worked with, both Sheffield based Asperger's Children and Carers Together, and Nottingham based Wheelbase Motor Project were merely warned by the ICO, that all laptops should be properly encrypted where they hold data. Whether an insurer would accept covering unencrypted laptops would need to be clarified but if declared and accepted then the breach of privacy could have been covered and the regulatory investigation costs as well. In November 2013 the International Business Times reported that a US children's hospital fundraising Charity called Extra Life was hit by a Distributed Denial of Service attack when it's website was taken down by hackers midway through their main annual online fundraising event. Again insurance could have responded positively to both cyber threats and extortion (if that was used), as well as costs incurred to reinstate the website and identify the perpetrators.

Could this happen to you?

The ICO has published details of data breaches within the Charity sector, as well as phishing scams causing public consternation where the scammers take money away from good causes. The City of London Police has identified around 1300 crime groups who use fraud as their means of making money[2]. With this as the backdrop the answer has to unfortunately be yes, with authoritative bodies such as the Charity Finance Group (CFG) recognising in a recent publication that whilst cyber risk may sometimes be seen as an issue affecting only larger Charities with large databases, any size Charity is actually affected as the numbers of records is irrelevant[3].

In their recent study[4], the Institute of Risk Management's Cyber and Information Management Special Interest Group found that organisations and risk professionals still underestimate the size, shape and nature of cyber risk, risk managers lack confidence in the subject matter and there is a naivety in response to risk. Their findings also highlighted nervousness around reporting breaches, a skills gap between the technology and cyber risk disciplines and weak governance hampering the ability to deal with technology.

The wealth of information on cyber risk is expanding rapidly, driven by requests for help and information from organisations within the UK, for example the ICO has issued a paper just for Charities on Data Protection and the Freedom of Information Act[5]. Sadly though there remains little guidance out there for Charities around hacking management, spoof website closure and how to withstand denial of service attacks on websites.

So what can be done?

Basically the same problems remain whatever type of cyber risk you have when you ask 'what are my cyber risks' and 'what can I do about them?'. A recent UK parliamentary report published by the House of Commons home affairs committee on e-crime indicated that good information assurance could solve 80% of cyber security vulnerabilities. By this the government wasn't referring to costly security measures but rather good IT housekeeping around keeping patches up to date, paying attention to personnel security and the education of users for each individual network.

So how do you measure up? Whether you are concerned about data protection issues, hacking, spoof websites or denial of service attacks, take our Arthur J.Gallagher Charities' Cyber Risk Healthcheck, to see how good your information assurance is.

Cyber Risk Healthcheck

Heading	Exposures		
Loss or theft of donor information from Charity's systems	Do you keep donor information electronically?	Yes	No
	Are donor credit card or bank details kept on your systems?	Yes	No
	Are these details encrypted?	Yes	No
	Do you have an IT policy in place regarding the handling of this type of data?	Yes	No
	Do you have a stable finance team?	Yes	No
	Do you use temps in your finance team?	Yes	No
	Do you update security software as soon as advised?	Yes	No
	Do you have a privacy policy in place governing your collection of private data?	Yes	No
	Are there automated checks and audit trails built into the financial systems?	Yes	No
	Do new supplier bank details need FD approval?	Yes	No
	Are checks made monthly on funds leaving the Charity's account?	Yes	No
	Are there flags set to highlight where and when donor information leaves the system?	Yes	No
Spoof websites – establishment of websites that may look and feel just like yours, but is taking funding away from you	Do you operate a website?	Yes	No
	Do you regularly check for spoof websites, e.g. using Google Alerts?	Yes	No
	Do you have a process in place if someone reports a spoof website?	Yes	No
	Have you discussed what to do with spoof websites with the Police?	Yes	No
	Have you discussed what to do with spoof websites with your Internet Service Provider?	Yes	No
	Have you been successful in identifying spoof websites to date?	Yes	No
Denial of service attacks on websites – resulting in you being unable to collect donations, sales invoices from retail operations, or just provide information to the people you want to help	Do you operate a website that provides you with an income or provides your beneficiaries with assistance?	Yes	No
	Are you PCI compliant?	Yes	No
	Do you have someone monitoring your website for attacks?	Yes	No
	Do you have a process in place if your website is attacked but the attack is not successful?	Yes	No
	Do you have a process in place if your website is successfully attacked/corrupted?	Yes	No
	Have you discussed what to do with your Internet Service Provider?	Yes	No
	Have you discussed what to do with the Police?	Yes	No
	Is there an established recovery process?	Yes	No
	Has the recovery process been successfully triggered before?	Yes	No
Loss of supporter data by third party suppliers/partners – whether by human error or deliberate act and the release of personal information relating to your supporters	Do you permit data to leave your system?	Yes	No
	Do you have a contract with a third party that clearly defines what they can and cannot do with your data?	Yes	No
	Do you conduct due diligence to ensure that the contract is being complied with?	Yes	No
	Are you certain that third party staff are all trained on Data Protection?	Yes	No
	Are you certain that third party staff are all employed and not temporary in nature?	Yes	No

How did you get on?

Whenever you have answered 'Yes' to the questions in red you have an exposure. If you have answered 'No' to these questions there is no exposure and no risk so provided that you are confident of your answer you can move on and ignore the questions in black under that heading.

Whenever you have answered 'Yes' to the questions in black, you have a control in place. However, whenever you answered 'No' to the questions there is a gap in your protections that should be addressed as quickly as possible.

Need more help?

Arthur J.Gallagher has worked with IT security specialists NCC Group to develop a packaged Cyber Risk Assessment for small and medium sized organisations, which in turn qualifies them for discounted cyber insurance. With costs starting at £3,500 plus VAT*, the risk assessment service includes:

- **Remote vulnerability scan**
  A remote scan of the internet (external) facing systems probing for vulnerabilities and unsecured access points. This will draw attention to the client's "open windows" in their IT Systems which are easy points of access by malicious outsiders.
- **High level cyber report**
  A traffic light (RAG) report on the overall security of the clients IT systems and the risks they face followed by succinct recommendations. The client can now assess their system vulnerabilities, business risks and take appropriate measures to mitigate against these.
- **One hour online meeting**
  An online meeting with a qualified Cyber Risk consultant for 1 hour to discuss the key findings and recommendations from the cyber risk survey and vulnerability scan of the clients systems. Ability for the client to ask questions about the report, overall cyber risk and understand the options for remedial action.
- **Incident response database**
  The client will be registered on the NCC Group's Incident Response data base where details of the IT systems and cyber posture are recorded. In the case of a system failure or external attack this will provide a handbook to the external consultants. Allows for a rapid response by external consultants with an existing knowledge of the clients business. Results in a more efficient process in rectifying the problem, saving the client time, effort and money.
- **One day onsite penetration test (ethical hack)***
  A low-level penetration hacking attempt at the client systems focusing on exfiltration (unauthorised release of data) of client details and personal data e.g. mimicking an outsider threat. Identifies high risk vulnerabilities in a clients system that is not possible to detect using automated software, and assesses the level of the potential business impact and costs.

* To include the onsite penetration test the cost increases to £6,000 plus VAT.

Insurance cover available

There are several specialist insurers that have developed Cyber insurance solutions for the not for profit sector, and protection does not need to break the bank, with cover starting from a minimum premium of just £250 plus Insurance Premium Tax at 6%.

Policies typically cover own out of pocket expenses as well as claims by third parties including:

- Cyber liability – your legal liability to pay third party claims against you arising from hacking attack or virus passed on by you or your cloud computing provider
- Privacy liability – your legal liability to pay third party claims against you due to a security breach
- Rectification costs that you incur in order to repair your own system damage
- Reduction in income due to a system outage as a direct result of a cyber peril, such as being hacked
- Consequential reputation harm from a cyber peril that reduces your income
- Legally permitted insurable regulatory actions and investigations including fines and penalties
- Privacy breach notification costs – including your own expenditure and when you incur cost in notifying third parties about the breach
- Cyber crime including computer cyber crime, such as unauthorised electronic funds transfers; identity theft due to fraudulent use or misuse of your electronic identity; cyber threats and extortion where a third party threatens to prevent you accessing your systems, introduces a virus, reveals confidential information, or damages your brand and reputation
- Telephone hacking for the cost of unauthorised calls being made by a third party
- Phishing scams whether by electronic communications or through your website including the cost of rectification, reimbursing people who are financially disadvantaged in good faith by the scam and any consequent reduction in income
- Multimedia liability and advertising injury – your legal liability to third parties for defamation, intellectual copyright infringement, invasion of privacy rights and content liability

The Arthur J.Gallagher Charities & Care Practice is experienced in designing the right cyber solution for you and we are happy to review existing insurance policy wordings to define to what extent, if any, your organisation is protected already through insurance.

Content was correct at the time of issue, but may have changed subsequently. If you are unsure please contact us.

FOR MORE INFORMATION CONTACT

T: 0844 332 0542
E: ukenquiries@ajg.com

www.ajginternational.com

Walbrook Office
The Walbrook Building
25 Walbrook
London
EC4N 8AW

About NCC Group

NCC Group is a leading global information assurance firm, providing freedom from doubt that all critical material is available, protected, and operating as it should be at all times. Information assurance is delivered through escrow and verification, security testing, audit and compliance, website performance and software testing services. NCC Group's security testing, audit and compliance services help mitigate the risk of malicious attack and data loss, and ensure the compliance of your processes with legal requirements. They deliver a highly respected, systematic and strategic approach, drawing on unparalleled experience and scale. With the world's largest penetration testing team and top level accreditations from bodies ranging from the government's CESG CHECK scheme to the PCI Security Standards Council, they are the trusted adviser to over 1,750 clients worldwide.

Sources and Additional Reading referenced in this bulletin

[1] Case Study One - Southern Daily Echo http://www.dailyecho.co.uk/news/10937687.Hoax_warning_as__scum__hack_Diabetes_UK_email/

Case Study Two - http://www.localgovernmentlawyer.co.uk/index.php?option=com_content&view=article&id=11984:charity-hits-out-at-ico-fine-fordata-breach-and-reserves-right-to-appeal&catid=54:childrens-services-articles

[2] http://www.channel4.com/news/criminals-internet-e-crime-fraud-mps-cyberspace

[3] Charity Finance Group (CFG) 'Protecting data, protecting people: A guide for charities' http://www.cfg.org.uk/resources/Publications/-/media/Files/Resources/CFDG%20Publications/Data_Protection2013.ashx

[4] The Institute of Risk Management's Cyber and Information Management Special Interest Group http://www.theirm.org/CyberRisk.html

[5] The Information Commissioner's Office "Data Protection and the Freedom of Information Act" (http://ico.org.uk/for_organisations/sector_guides/charity),