Computer Hacking, The Invisible Threat

by Helen Murphy

In this article, Helen looks at what policies and procedures accountants need to have in place to ensure safe online practice and to provide training to staff.

What do Jeff Bezos, Jackson County, Georgia, Riviera Beach, Florida and HBO all have in common?

They have all been hacked and suffered financial loss as a result.

In Jeff Bezos' case, hackers got access to his iPhone, including his photo albums, which contained pictures of Mr Bezos with another woman while he was still married. His resulting divorce settlement cost him €38 billion in Amazon stock.

Jackson County, Georgia was held to ransom by hackers who took control of its computer systems. A €400,000 ransom payment was required to regain control whilst Riviera Beach, Florida had to pay €600,000 to regain control of its systems. Hackers demanded €7.5 million from HBO to prevent the early release of scripts and episodes for shows such as Game of Thrones.

In July 2015, Ashley Madison, the self-described "cheating" website was hacked, with the personal data from all its users copied. Over 25 gigabytes of data was leaked over two days in August which included real usernames, addresses and emails. Needless to say, this caused consternation for members and at least 2 suicides have been linked to the hack.

The cases above are just scratching the surface when it comes to the cybercrime incidents that have occurred over the last couple of years and while the Jeff Bezos and Ashley Madison case grabbed the headlines, the other cases mentioned above were very costly for the organisations involved.

We now provide our personal data on almost a daily basis to a variety of organisations. Providers of services are adept at getting us to sign up for accounts with them whether it is for special offers via emails, discount coupons or simply so that they can provide a receipt in respect of a purchase we have made. While the thought may fleetingly cross our mind that this may not be a good idea, the carrot dangled in front of us may be too tempting to pass up on.

And of course, we trust that the organisation handling our data will look after it. As we can see, this is not always the case.

But what if you're not the individual whose information is hacked? What if you're the organisation that ends up being hacked and as a result, sensitive, personal and financial information that you hold on your clients ends up in the public domain? How do you deal with the resulting reputational damage, as well as the cost of undertaking a forensic review of your systems to ensure it doesn't happen again?

And before you think "why would anyone want to hack my systems, I'm just an accountant"? – read on.

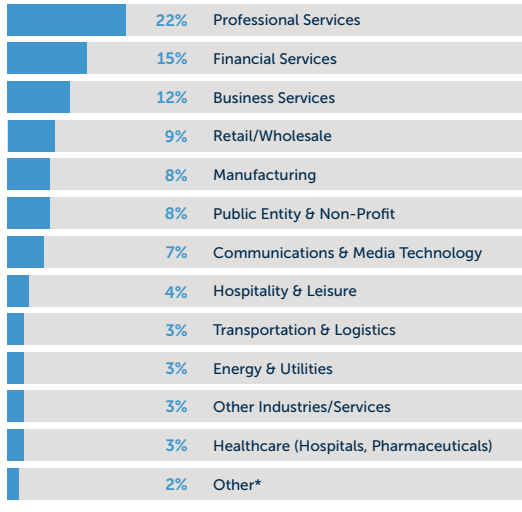
Cyber Insurance and Data Protection for Accountants

Cyber threats are a growing risk for Accountants both in Industry and Practice. The reason Accountants are particularly attractive for a cyberattack is due to the amount of sensitive financial data that they hold. In fact, it is estimated that financial institutions are over 30% more likely to be targeted than other companies.

Most businesses believe they are not at risk as it is only the household names that make cyberattacks newsworthy. However, the majority of attacks are against small businesses. If a business collects and stores customer information, payment information or personal health records there is a risk to the business of a data breach. Most companies will not be immediately aware that a breach has occurred and the longer a breach goes unnoticed the higher the number of records that can be obtained. In addition to a financial loss, the business will suffer a loss of trust with their clients and reputational damage.

As can be seen from the AIG cyber claims statistics below, a high level of cyberattacks are perpetrated on professional and financial services businesses:

Cyber Claims received by AIG EMEA (2018) - By industry



* Food & Beverage, Construction
Note: Figures may not add up to 100% due to rounding

Previously the main risk of a data breach was through loss or theft of physical data held. Now with data being stored electronically, data can be accessed in a number of ways. In 2018, as can be seen from the AIG report below on cyber incidents by type, business emails compromised in the form of hacking and phishing is the most common type of security breach. This is followed by ransomware through which your computer system is effectively hijacked and only released back to you on payment of a ransom, with data breaches by hackers and as a result of employee negligence being the other main types of incident in 2018.

Examples of common incidents that occur are:

- The files of the business unexpectedly become encrypted and a ransom demand from a hacker arrives. Systems are unavailable until the ransom is paid.
- A staff member leaves their work laptop on public transport which contains personal data resulting in notification requirements under GDPR.
- An employee of a firm makes a bank transfer of €25,000 to fraudsters after receiving a phishing email supposedly from a senior manager.

Cyber Claims received by AIG EMEA (2018) - By report incident

23%	Business Email compromise
18%	Ransomware
14%	Data breach by hackers
14%	Data breach due to employee negligence (e.g. sending data to the wrong person)
8%	Impersonation fraud
6%	Other virus/malware infections
5%	System falure/outage
3%	Physical loss or theft if information assets (e.g. stolen laptop)
4%	Other*
3%	Other cyber extortions (non-ransomware)

* Denial of Service Attacks. Legal/Regulatory Proceedings based on violations of data privacy regulations

What costs associated with cyber-crime would be covered by my PII policy?

Take the example of a hacker gaining access to an accountant's systems and obtaining details of a number of clients. The hacker then threatens to post the information online unless a ransom is paid.

The financial loss would be the ransom, costs incurred through the forensic investigation of the breach, credit monitoring costs for clients or third parties impacted, public relation costs to reduce reputational damage to the accountant, and support in notifying the incident to the Data Protection Commissioner's Office and all impacted clients.

The professional indemnity insurance policy would not provide indemnity for ransom costs, forensic investigation, public relations, costs associated with notifying the Data Protection Commissioner or the loss of income due to the business interruption.

Traditional insurance policies are not designed to deal with 21st century threats, as most insurance policies deal with the loss of physical assets. The world has changed and the threat to digital assets is growing.

So, what can you do to protect your business?

Prevention is better than cure in all circumstances, therefore accountants need to have policies and procedures in place to ensure safe online practice and to provide training to staff. There also needs to be procedures in place for dealing with breaches.

The following list (while not exhaustive) will certainly help:

- Train your employees on cyber security.
- Raise workforce awareness and accountability.
- Improve communications and engagement with the board of directors.
- Align security to business goals.
- Boost cyber resilience.
- Be proactive in compliance.
- Keep pace with innovation.
- Engage security experts at the start of digital transformations.
- Purchase a cyber and data protection policy.

Learn more about Cyber Insurance cover by contacting Helen at helen@jdminsurance.ie

"The world has changed and the threat to digital assets is growing."

Helen Murphy,
Managing Director,
JDM Insurance Services Ltd