Brown & Brown

Volume 10, Issue 1

Cyber Matters

Feb 2025, Brian O'Mara

10 years of Cyber Matters

This is the tenth year of our newsletter and the first since our rebrand to Brown & Brown. In this issue we take stock of the cyber-security environment for Irish businesses, and look at what actions businesses can take to manage this ever-evolving risk.

Some things haven't changed. In our first edition we talked about companies falling victim to fraudulent bank transfer instructions, and an accountant being locked out of their systems by 'encryption'; ransomware in 2025 parlance. We also referenced that GDPR was just two years away – hard to imagine it is now nearly six years old!

Some risks have fallen off our radar. We're not sure if people losing money to hackers re-routing toll calls through company phones is a thing of the past, but it's not something we have come across since the early days of our newsletter. This is likely due to better monitoring by the phone companies.

Some issues from 2016 seem almost innocent – on page 1 of our first ever issue we mention customers suffering 5-figure losses. Unfortunately, the trend quickly increased to 6-figure losses, and later in this issue we have a case study of a recent large **7-figure loss to a customer.**

Cyber Threats Are Evolving—Is Your Business Prepared?

There is increased public awareness around the likelihood of a business suffering a cyber-incident compared to back in 2016. However, even we were surprised at some of the data around this. It is important to be aware of the likelihood of a cyber incident and figure out what you can do to try and prevent it affecting your business.

An Expleo report from August 2024 surveyed over 200 Irish companies, each with over 50 employees. Somewhat astonishingly, 31% have set aside monies to pay ransoms. **33% had already paid ransoms** within the 12 months prior to the survey.

This echoes research from Aviva in the UK, wherein they stated that **10% of small businesses and 20% of businesses more generally had experienced a cyber incident or attack** in the preceding 12 months. Aviva supports this data by suggesting that cyber-attacks are almost **5x more likely than a fire and 67% more likely than a theft.**

Are You Investing Enough in Cybersecurity?

Each business is different, but as a starting point you should consider the below:

Consider:	Cost:	Where to Start?
Are we spending enough on our IT/ cyber-security systems?	€ - €€€	Talk to your IT provider/ team
Do we train our staff, and practice what we preach in terms of cyber security?	Free - €€	Free resources such as the Jigsaw phishing quiz (search online). Paid – utilise the services of cyber-security companies
Do we have an up-to-date Incident Response plan, which includes responding to a cyber-attack?	Free - €	Either look up templates online, or speak with your IT provider / team
Have we explored cyber insurance options to strengthen our risk management strategy?"	€ - €€	Across hundreds of our customers the median Cyber insurance premium is €4,410. Those premiums start in the hundreds of euros.

Case Study – Large Sophisticated Cyber-Crime Loss

Last year, an Irish business experienced a devastating cyber-related financial loss **exceeding seven figures.** Despite being a relatively small company, it fell victim to a highly sophisticated attack that resulted in substantial monetary theft. The impact was severe—most of the stolen funds were never recovered, leaving the company in a precarious financial position. **Without the necessary safeguards in place, this kind of incident can be catastrophic.**

Before we get into the detail of what happened, it is worthwhile giving some wider context to how common these incidents are.

- Engineering firm ARUP lost £20m to a deepfake / AI fraud last year.
- A 158-year old UK-based logistics firm, which was very much cyber-security aware, had to enter administration in 2023 after a ransomware attack.
- In October, the Banking & Payments Federation Ireland (BPFI) warned consumers of a new ‘direct-debit’ scam used similar techniques to the case study below on individuals.

So What Happened, and Can We Learn Lessons From This Incident?

The loss in question was a voice-based phishing attack. The whole ploy was very convincing.

Tuesday

- Our customer was contacted by phone by people claiming to be from their bank. The malicious actor had an Irish accent and presented various details to reassure the customer that they were from the bank in question, for example they knew details such as the company's bank account number.
- The criminals mentioned a suspicious transaction on the account, as if they were acting in their interests protecting our customer, and they ended the call suggesting that the customer check all transactions.

Thursday

- The next step of the ruse was for another individual professing to be from the bank to call our customer again a couple of days later, quoting the account number and a case reference number they had created. They told the customer they had to do a profile reset. Our customer was transferred to someone purporting to be from IT. Both of these individuals also had Irish accents; in the mind of our customer, this is now a genuine call with their bank.
- The 'IT' team shares a website link with the customer. When opened, it looks like a genuine bank website.
- During this chat, IT extracted the online login codes from the customer. They now have the information they want to access their bank account.
- The criminals say that the reset will take 24-48 hours to go through. This reassures the customer and they don't check their bank account during this time as a result.

Friday

- The criminals are using this time to transfer funds out of the account. All the while, they are ringing our customer and gaining access to the approval codes for transfers, under the guise of it being part of the reset of their account.
- Later on Friday, the bank contacts our customer flagging unusual activity – several transactions across Thursday and Friday. At this point the reality of what had happened hit.

Across numerous transactions, a very large sum of money was transferred. The total loss was over **€1 million.** Some funds were recovered, but the vast majority has not been, nor is it likely to be.

What stands out is how easily this could happen to anyone. This was a very targeted and catastrophic loss to a small business. One can only imagine how sophisticated and convincing this crime was in real time, and without the benefit of hindsight. In relation to the direct-debit fraud mentioned earlier in the piece, the BPFI commented that:

"These fraudsters can be very skilled at convincing people and gaining our trust, using a variety of psychological techniques known as 'social engineering', so it's possible for any of us to be caught out if we're not on alert" .

Thankfully, the company in question survived, primarily because the majority of the loss was covered by their cyber insurance. **Would your business have the resources to help mitigate the impact of a similar attack?**

How to Protect Your Business Now

Tips from the BPFI to protect yourself from phone and text scams:

- Do not reply to unsolicited text messages or provide personal or financial information.
- Do not use phone numbers provided within the text of a text message. Contact your bank using the number on the back of your debit / credit card.
- Do not click on a link from unsolicited text messages - remember your bank will never send you a link in a text message.
- If someone is pressurising you on the phone to take urgent action, hang up and call the number on the bank of your debit / credit card.
- Never give away personal information, bank card payment details, bank account details or security details such as your PIN or online password to anyone.

Source: Consumers warned of new 'direct debit' scam on the rise.

Real Stories, Real Losses.

- We had a recent occurrence where an estate agent had to refund a **€20,000** deposit back to a customer. However, cyber criminals took advantage and the company in question did not verify the bank details. The funds were sent to a fraudulent bank account. Their insurance policy paid out on the claim.

- Another customer in the leisure space was hacked. This resulted in customer card details being stolen. The initial loss was for one individual for a few hundred euro. However, on further investigation up to 1,000 customers may have been affected and they had to be contacted. The cost of this incident is not yet finalised but will be in the **tens of thousands.**

These are not just cases - they are realities. Cybercrime isn't going away, the question is, **have you protected your business against the risk?**

Brown & Brown

Ready to find your solutions?
Let's Chat.

Brian O'Mara, *ACII*
Account Executive
brian.omara@bbrown.com