

# Cyber Matters Newsletter

## July 2024

Welcome to our July Cybersecurity Newsletter! This month, we delve into recent high-profile breaches, explore emerging threats, and offer expert insights on fortifying your digital defenses.

### High-Profile Cyber Attacks in 2024

The year 2024 has seen several high-profile cyberattacks targeting diverse sectors, highlighting the growing sophistication and reach of cybercriminal activities.

**Ticketmaster**, the global ticket sales and distribution giant, faced a significant cyberattack in early 2024. Hackers infiltrated their systems, compromising customer data including payment information and personal details. The breach disrupted services worldwide, causing massive financial losses and raising serious concerns about the security of online transaction platforms.



The renowned Belgian brewery, **Duvel**, also fell victim to a cyberattack this year. The breach disrupted IT systems, impacting production and distribution processes. Cybercriminals accessed sensitive corporate data, threatening to leak proprietary information unless a ransom was paid. This incident underscored the vulnerability of the beverage industry to sophisticated cyber threats.

In a disturbing attack, hackers targeted a **care home in Leicester**, accessing sensitive medical and personal records of residents. The breach compromised the privacy and security of vulnerable individuals, highlighting the urgent need for enhanced cybersecurity measures in healthcare facilities to protect against such violations.

The global engineering and consulting firm **Arup** experienced a cyberattack that infiltrated their network, exposing confidential project data and client information. The breach not only disrupted business operations but also posed significant risks to the integrity of critical infrastructure projects worldwide.

These incidents collectively emphasize the critical need for robust cybersecurity strategies across all sectors to protect against evolving cyber threats in 2024.

Thanks for reading. If you have queries on Cyber or any other insurances feel free to contact us on [cyber@oli.ie](mailto:cyber@oli.ie).

# Cybersecurity Breaches Highlight Vulnerabilities in Irish Institutions

Recent investigations into potential cybersecurity breaches at the Department of Foreign Affairs (DFA) in Ireland and a costly ransomware attack on Munster Technological University (MTU) underscore the critical need for robust cybersecurity measures in both public and academic sectors.

## Potential Breach at the Department of Foreign Affairs

The Department of Foreign Affairs in Ireland is currently under scrutiny for a potential cybersecurity breach. Details of the breach remain sparse as the investigation unfolds, but the incident has raised serious concerns about the security protocols protecting sensitive governmental data. This breach could have significant implications, potentially compromising diplomatic communications and classified information.

## BLACKCAT Ransomware Attack on Munster Technological University

Meanwhile, Munster Technological University recently faced a devastating ransomware attack attributed to the BLACKCAT group. This attack has resulted in a substantial financial impact, costing the university approximately €3.5 million. The BLACKCAT ransomware, also known as ALPHV, is notorious for its sophisticated techniques and ability to evade traditional cybersecurity defenses.



The attack on MTU disrupted operations, leading to the temporary shutdown of IT systems and significant data loss. The recovery process has been both time-consuming and expensive, highlighting the financial and operational vulnerabilities exposed by such cyber threats.

## The Growing Threat Landscape

These incidents reflect a broader trend of increasing cyberattacks targeting critical infrastructure and institutions. As cybercriminals employ more advanced tactics, the repercussions of breaches are becoming more severe. For educational institutions like MTU, the financial strain of recovery is compounded by the potential long-term damage to reputation and trust.

## AI is everywhere...even here!

So, we have a confession to make...this edition of our newsletter has been a bit of an experiment. Everything you have read to this point has been drafted using Chat GPT!

We gave Chat GPT the prompts (e.g. *'High profile cyber attacks in 2024 - 200 words - Ticketmaster, Duvel, Leicester care home, Arup'*), and the software did the rest. We have not edited a word, it is presented as it came out. Be honest – did you notice?



### (AI free) Note from the Editor

As with other technological advances, AI is already bringing both challenges and opportunities to Irish businesses. At a minimum, business owners and leaders need to understand how AI can affect their operations.

- Employees need training on risks associated with AI. Many companies are creating rules about when Chat GPT can be used by employees. A crucial part of this is not to come up with a procedure and have it gather dust; reinforcement is key.
- Companies are already figuring out how AI can be used as a benefit to them. It could be as simple as automating mundane tasks, to harnessing AI to generate more sales for your business.

From an insurance perspective, it is important to understand how you might be covered for issues related to AI. Have a conversation with your insurance broker to chat through the following:

- 1) What are the risks to your business?
- 2) Is your insurance program adequate if there is an issue?
- 3) If there is a gap, understand what insurance is available. Be informed enough to weigh up any additional cost against the benefits it brings to your business.

As always, we are here to help!

Please note, no human was replaced in the making of his newsletter—normal service to resume in 2025! However it is an eye opener to see just how impactful the software can be....

The case studies mentioned on the last page are AI-free, we promise...

# Cyber Matters Management Newsletter

Thank you for reading our newsletter. Below are links to our own social media pages. Follow these to keep abreast of important updates.

LinkedIn: <https://goo.gl/u06ncG>

Twitter: @OLearyInsurance

Facebook: <https://goo.gl/DILziV>

## Recent case studies of cyber incidents from our client base



### Phishing attack

An employee opened an attachment on an email that appeared to be genuine, however it was fraudulent. The manufacturing company in question had to shut down their systems and recover their files from their backup, causing interruption to their business. Back-ups can quite often be missing key data, so it is worth testing these a couple of times each year.

### Ransomware attack

A sophisticated ransomware attack took down the back-ups of a consulting engineering firm. The company had an offsite backup that they could work from, however not all data was saved so much of it had to be re-created.

### Clients of company lose monies

Our client was hacked. The hackers contacted some of their customers, choosing ones that were due to transfer funds. Over €100,000 of customer funds were lost.



Office	Contact	Phone	Email
Cork	Brian O'Mara	021 453 6860	<a href="mailto:bomara@oli.ie">bomara@oli.ie</a>
Dublin	Carman Devlin	01 663 0604	<a href="mailto:cdevlin@oli.ie">cdevlin@oli.ie</a>
Galway	Brendan Devlin	091 454 042	<a href="mailto:bdevlin@oli.ie">bdevlin@oli.ie</a>
Waterford	Fiona Fitzgerald	051 309 130	<a href="mailto:ffitzgerald@oli.ie">ffitzgerald@oli.ie</a>

**About O'Leary Insurances – Insurance Brokers & Consultants**

From an initial complement of three staff in 1961, originally founded by Archie O'Leary, O'Leary Insurances has successfully grown & developed into an Insurance Brokerage which specialises in providing a high level of customer service throughout Ireland. The O'Leary Insurances group of companies are all wholly owned subsidiaries of Brown & Brown, Inc. one of the largest and most respected independent insurance intermediaries in the United States of America (NYSE BRO). You can find out more about us at [www.olearyinsurances.ie](http://www.olearyinsurances.ie).

Cyber Risk is now recognised as a top threat to all types of businesses. We at O'Leary Insurances were quick to realise the potential risk to our clients, and have acted accordingly. We have recruited and researched so that we can advise and provide our clients with up-to-date details of the exposure, and our ability to engage with organisations in this space is only possible because of our determination to do everything we can to protect our clients.

Our highly trained and experienced personnel would be delighted to be of service to you and would welcome the opportunity to discuss both your Personal Insurance and Business Insurance requirements with you. We are confident that our knowledge and expertise can assist you in the management of your insurance needs and can assure you of our very best attention in meeting the challenges of the future.

**Disclaimer – as insurance brokers we cannot provide legal advice. Thank you for reading.**

