Below are extracts from a range of cyber security articles, published by The Financial Times (ft.com 17th January 2024), RTE.ie (21st February & 6th March 2024) and Breakingnews.ie (21st February 2024) as referenced below.

A focus on Cybersecurity and the rise of cyber-attacks globally.

With 'Zero Day Con' Cyber Convention taking place in Dublin this week and the recent success of our Seaspray Private's Cyber Security Bond the focus of our news this week is on the highly topical area of cybercrime.

JPMorgan suffers wave of cyber-attacks as fraudsters get more devious.

In his recent Financial Times report, Walker, O. (2024) reveals how Mary Erdoes, JP Morgan's head of asset and wealth management, while at the 54th World Economic Forum in Davos, detailed the bank's current wave of cyber security attacks. Much of JP Morgan's investment in technology is currently geared towards combatting cyber-crime, but the task is becoming increasingly difficult as hackers get smarter and more devious:

> JPMorgan Chase is suffering a wave of cyber-attacks as fraudsters get "smarter, savvier, quicker, more devious, more mischievous", the bank's head of asset and wealth management has said.
>
> Speaking at Davos on Wednesday, Mary Erdoes said the bank spent $15bn on technology every year and employed 62,000 technologists, with many focused solely on combating the rise in cyber-crime. "We have more engineers than Google or Amazon. Why? Because we have to.
>
> The fraudsters get smarter, savvier, quicker, more devious, more mischievous," Erdoes said. "It's so hard and it's going to become increasingly harder."
>
> "Examples of activity can include user log ins like employee virtual desktops, and scanning activity, which are often highly automated and not targeted," the bank added. Western lenders have suffered a surge in cyber-attacks in the past two years, which has been partly blamed on

> Russian hackers acting in response to sanctions placed on the country and its banks following its full-scale invasion of Ukraine.
>
> Walker, O. (2024)

According to Walker, O. (2024), the International Monetary Fund(IMF) is concerned about the increased impact of AI on cyber security in the banking sector. Specifically, from the point of view of the behaviour of financial markets, data privacy and a potential bias in lending decisions:

> The use of artificial intelligence by cyber criminals has also increased the number of incidents and level of sophistication of attacks. Last year, the number of ransomware attacks in the finance industry surged by 64 per cent, and was nearly double the 2021 level, according to Sophos, a cyber security company.
>
> JPMorgan was the victim of one of the biggest cyber attacks on a bank a decade ago when the data on 83mn accounts — including 76mn households and 7mn businesses — were compromised. Speaking at the same Davos event, Gita Gopinath, deputy managing director of the IMF, said the use of AI by cyber criminals was raising concerns for policymakers. “Given the tremendous uncertainty about the scale of the impact of this technology and the way it is evolving, policy could be playing catch-up,” she said. “We could risk having a big event before we actually work out how to fix it.” Gopinath said banks were among the biggest spenders on AI technology and that while there were many benefits for them in terms of improving productivity, there were also risks concerning data privacy and embedded bias in lending decisions. She added that the IMF was also concerned about the long-term risk of AI affecting the behaviour of financial markets.
>
> “If we enter a world where all major banks are using this technology, which is being produced by three or four big companies, are we going to see supercharged herding behaviour, where AI bots or models are sentiment-driven and feed off of each other? “You then end up with much bigger amplitudes in the financial cycle — you get big credit booms and big credit busts. This is something we are looking into.”
>
> Walker, O. (2024)

Spike in malware designed to steal personal information.

Meanwhile in an article in recent weeks, RTE (2024) explains how there has been a 71% global spike in cyber-attacks involving stolen identities, according to IBM and stresses that the advances in artificial intelligence could make the situation even worse :

> There has been a 71% global spike in cyber-attacks involving stolen identities according to IBM. Its latest X-Force Threat Intelligence Index found there was a growing trend in 2023 of cyber-criminals logging into corporate networks using stolen credentials as opposed to hacking into systems.
>
> The report is based on insights and observations from monitoring over 150 billion security events per day in more than 130 countries. It found there was a 12% drop in ransomware attacks last year with larger organisations often refusing to pay hackers and instead choosing to rebuild their infrastructure.
>
> IBM said that in 2023, attackers increasingly invested in operations to obtain users' identities with a spike in malware designed to steal personal information such as email, social media, and messaging app credentials as well as banking details and crypto wallet data.
>
> The report's authors are warning that advances in artificial intelligence could make the problem worse.
>
> RTE (2024)

Biden to launch cybersecurity rules for US ports amid vulnerability concerns.

In Breakingnews.ie article, Long, C. (2024) brings us news of a move by the Biden administration in the to tighten and heighten cyber security regulations at its major shipping ports, in light of increased vulnerability to spying and ransomware attack:

> US president Joe Biden is expected to launch new regulations aimed at better securing US ports from potential cyberattacks. The administration is outlining a set of cybersecurity regulations that port operators must comply with across the country, not unlike standardised safety regulations that seek to prevent injury or damage to people and infrastructure.
>
> "We want to ensure there are similar requirements for cyber, when a cyberattack can cause just as much if not more damage than a storm or another physical threat," said Anne Neuberger, deputy national security adviser at the White House. Ports across the US employ roughly 31 million people and contribute 5.4 trillion dollars to the economy and could be left vulnerable to a ransomware or other brand of cyberattack, Ms Neuberger said.
>
> Long, C. (2024)

Long, C. (2024) notes the absence of a nationwide set of standards for port operators, which is a growing concern for the US government, given its role in the country's critical infrastructure . Also, this move is a reaction to the ever- increasing role of hostile cybercrime in geopolitical rivalry around the globe:

> In 2021, the operator of the largest fuel pipeline in the US had to temporarily halt operations after it fell victim to a ransomware attack in which hackers hold a victim's data or device hostage in exchange for money. The company, Colonial Pipeline, paid 4.4 million dollars to a Russia-based hacker group, though Justice Department officials later recovered much of the money.
>
> Ports, too, are vulnerable. In the US, roughly 80% of the giant cranes used to lift and haul cargo off ships onto US docks come from China, and are controlled remotely, said Admiral John Vann, commander of the US Coast Guard's cyber command. That leaves them vulnerable to attack, he said.
>
> Long, C. (2024)

As referenced, Ireland is doing its bit this week in the fight against cybercrime, hosting the **'Zero Day Con' Cyber Convention** in Dublin, and RTE (2024) outlines the theme of the conference, 'Evolve', reflecting "how the cyber environment is constantly changing particularly when it comes to the ever-increasing number and type of threats facing organisations at all levels." The conference features speakers in the fields of industry, law enforcement, medicine, and education.

References

Walker, O. (2024) 'JPMorgan suffers wave of cyber-attacks as fraudsters get 'more devious'. *Financial Times January 17*. Available at: https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962?accessToken=zwAGD3m6C0SAkdPNKHNSyztI2NOoW2aHE7gJYg.MEQCIBOqt7SPSLfr8hdO_h2CHjSGcQLmiJVYIvGgfelFpQCMAiAIrFqpMfMm9i52SwF7PY13VtKmiFK54uMnw42VzF8o_Q&sharetype=gift&token=772281a0-a198-4433-b8f4-728d6a88508a . (Accessed 26 February 2024).

RTE (2024) 'Big jump in cyber-attacks using stolen identities – IBM'. *RTE.ie February 21*. Available at https://www.rte.ie/news/2024/0221/1433449-cyber-attacks/ (Accessed 01 March 2024).

Long, C. (2024) 'Biden to launch cybersecurity rules for US ports amid vulnerability concerns. *Breakingnews.ie February 21*. Available at https://www.breakingnews.ie/world/biden-to-launch-cybersecurity-rules-for-us-ports-amid-vulnerability-concerns-1591614.html (Accessed 26 February 2024).

RTE (2024) 'Cybersecurity experts gather for Dublin convention'. *RTE.ie March 06*. Available at Cybersecurity experts gather for Dublin convention (rte.ie). (Accessed 06 March 2024).

EON- 05-03-24