The cost of cybercrime 2022

Irish Cybercrime expected to exceed €10 Billion in 2022

A year in time - where are we today?

One year ago, Grant Thornton published the "The Economic Cost of Cybercrime" report. It was apparent then that Irish businesses were extremely vulnerable to cybercriminals, and that they needed to focus their planned cyber security investments on the ability to detect and react to data-security breaches. It was not a question of 'if' an Irish business will be the victim of a cyber-attack but a question of 'when'. Businesses needed to act, and build their internal capabilities to prepare for attacks.

2021 was the year when Ireland faced its' cyber "Annus Horribilis", where a major Ransomware attack on Ireland's National Health Service Executive (HSE) brought the impact of cyber-attacks home to a significant proportion of the Irish population.

Trends from 2021 have continued, and in some cases accelerated, over the last year and Ireland is more vulnerable than ever to cyber-attacks. This is in part due to the increase in both remote and hybrid working, alongside continued Ransomware threats and a criminal focus on exploiting supply chains. Compared to their European Union counterparts, there are indications that Ireland is not dealing with these threats as effectively.

Cost to Businesses

The Association of Compliance Officers Ireland conducted a survey in 2021, which showed that 65% of Irish companies consider remote working and the threat of cyber-attacks as the number one data-protection concern. The survey's main objective was to understand the current data-protection risks facing companies within Ireland. The results indicated that 85% of respondents have more than 75% of their workforce working from home in 2021.

Another survey conducted by the European Commission disclosed that one in three Irish small to medium enterprises (SMEs) fell victim to cybercrime between May 2021 and April 2022. Further, 12% of respondents who were a victim of ransomware paid the fee; translating to double the EU average rate of ransom payments. The Irish Examiner[1] also reported that one in three of Ireland's SMEs paid out money to cybercriminals, with the average ransom payout being €22,773. Of the 200 SMEs that were surveyed and disclosed their payment, almost three-quarters (74%) said they have done so on multiple occasions.

Cost to Government and Individuals

Phishing activity has been a significant contributor to successful cyber-attacks in recent years. The Garda's National Cybercrime Bureau (GNCCB) recorded a 22% increase in cases through 2021 while noting that current backlogs extend to an estimated three-years. While delivering the latest statistics on the subject, Minister for Justice, Helen McEntee, said the number of cases taken on by the Garda National Cyber Crime Bureau (GNCCB) increased from 400 in 2020, to 490 in 2021[2] translating to a 22.5% increase. In addition, 2022 has demonstrated an increase of 111% in overall fraud instances when compared with 2020, alongside a 370% increase in fraud-related crimes made up of vishing (fraudulent phone calls), smishing (fraudulent texts) and phishing (fraudulent emails)[3].

[1] https://www.irishexaminer.com/business/technology/arid-40968995.html#:~:text=A%20third%20of%20Ireland's%20SMEs,leaked%20into%20the%20public%20domain

[2] https://www.irishexaminer.com/news/courtandcrime/arid-40888037.html

[3] https://www.joe.ie/news/scam-calls-texts-emails-ireland-741604

Major Cyber Events of 2021

Ransomware

The number of significant ransomware attacks in 2021 meant it became a topical board level item. On May 7, 2021, a ransomware cyber-attack breached an American oil pipeline system, impacting their computerised pipeline management. One of Ireland's largest ransomware attacks on a public entity in 2021 targeted an Irish Health Service provider. This cyber-attack cost taxpayers at least €101 million, while upwards of €657m will be spent on upgrading the organisation's IT systems to safeguard against repeat attacks. €17m was spent on professional services including cyber security, €14m was allocated for hospitals' cyber costs, €13m was spent on replacing IT devices and €7m went towards other costs such as Office 365 packages and cloud-based systems. The attack itself saw massive disruption across the country, with IT outages curtailing healthcare operations.

System Vulnerabilities

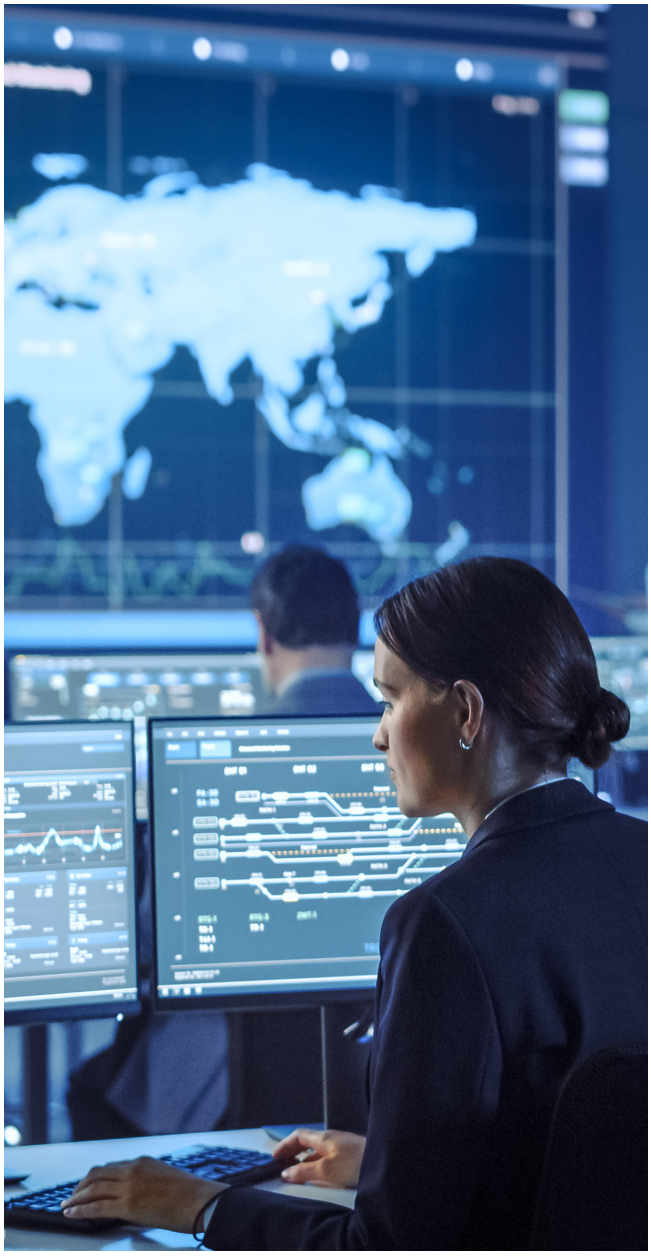
In December 2021, the National Cybersecurity Centre (NCSC) of Ireland also reported another major vulnerability in the form of Apache Log4j (CVE-2021-44228)[4]. According to the NCSC, the issue only affected organisations' operating web server infrastructure, and not people browsing the web on laptops or personal devices. Nevertheless, the vulnerability was widespread and used by major organisations across all sectors of industry. Primarily, the threat affects the organisations rather than individual legitimate users who may access resources relying upon log4j. Almost one full year later, the vulnerability persists without the released patches upon servers that are now trivial to identify. Correspondingly, the embedding of log4j libraries may be classified as a supply chain risk.

Cryptocurrency attacks and fraud

Cryptocurrency has also been extensively utilised in cybercrimes and criminals are increasingly using it to evade law enforcement and Anti-Money Laundering (AML) measures. This heightens the challenge for law enforcement to track and trace cryptocurrency payments to cyber criminals. According to the Microsoft Digital Defence Report 2022[5], worldwide spending on blockchain solutions grew by approximately 340% over the last four years, while new cryptocurrency wallets grew by around 270%. There are more than 83 million unique wallets globally, and the total market capitalisation of all cryptocurrencies was approximately €1.07 trillion as of July 28, 2022. Interestingly, cyber-attacks on cryptocurrency exchanges has become commonplace while the biggest story of the year stemmed from the collapse of FTK exchange. FTX collapsed in early November 2022 following a report by Coin Desk highlighting potential leverage and solvency concerns involving trading firm Alameda Research. Within hours of filing for bankruptcy, FTX said it was the victim of "unauthorized transactions" and would move its digital assets to cold storage for security purposes. Outside analysts said they suspect that about €465 million was stolen from FTX in the suspected hack.[6]

Malware and Russian invasion

The European Union Agency for Cybersecurity (ENISA) highlights that after the COVID-19 drop, malware is on the rise again. 2020, and the beginning of 2021, saw a global decrease in malware. This drop was linked to the COVID-19 pandemic and employees worked from home, thus limiting the visibility of malware infections as may be typically found upon corporate infrastructures. However, by the end of 2021, when more people started returning to the office, there was a notable increase in malware. The immediate and subsequent aftermath of Russia's invasion upon Ukraine saw a further increase in detected malware. Threat actor groups have declared alliance to either nation and vowed to attack any entity who dares to try attack their favoured country.



[4] https://www.ncsc.gov.ie/pdfs/apache-log4j-101221.pdf

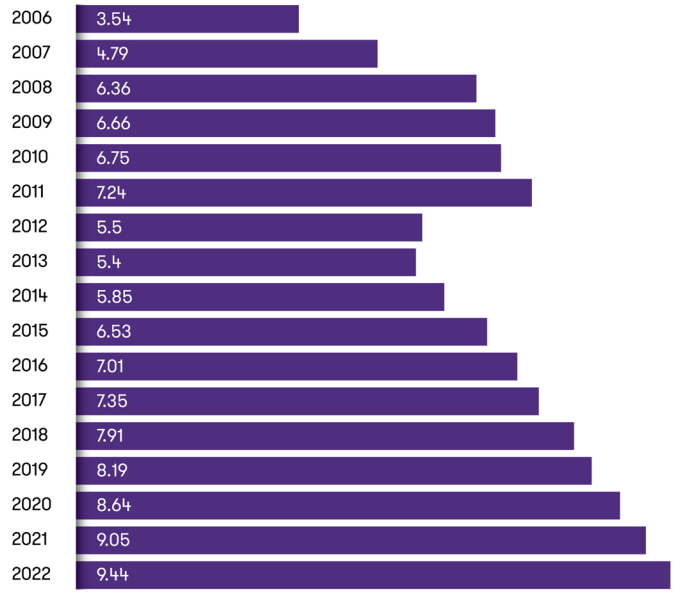
[5] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

[6] https://www.investopedia.com/what-went-wrong-with-ftx-6828447

Global Impact

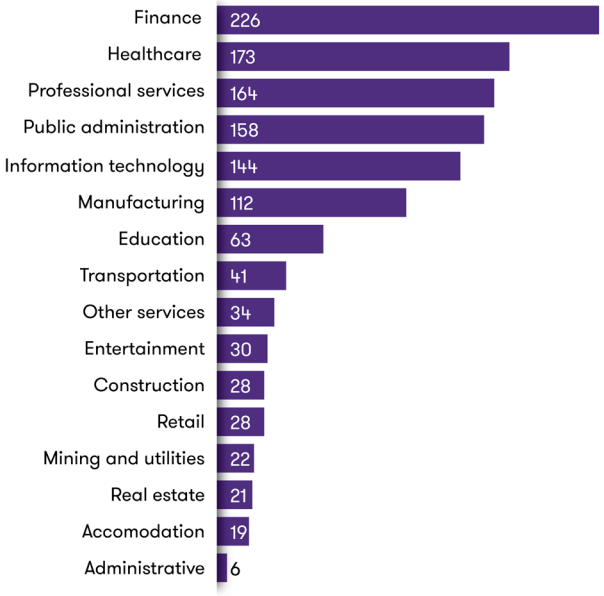
On a larger scale, the economic cost of cybercrime has been on a sharp rise worldwide in different industries as evidenced by the Grant Thornton LLP research on cyber security internal audits[7] and represented in the graphs below:

Average cost of a data breach in the U.S. (in million of U.S. dollars)



Source: Statitsta

Sectors most targetted by basic web application attacks worldwide (November 2020 to October 2021)



Source: Statitsta

The COVID-19 pandemic has amplified of existing threats exploiting the uncertainties characterising the pandemic. According to the ENISA threat landscape 2021, during COVID-19, Ransom Denial of Service (RDoS) or extortion by Distributed Denial of Service (DDoS) had a 67% increase above those recorded in July/August 2020, mostly targeting businesses in the e-commerce, finance, and travel sectors on a global scale. This trend continues to materialise in 2021-2022.

Phishing campaigns follow trends or major events, as evidenced by statistics compiled and reported by SC Media, (November 2022). The World Cup soccer tournament launch in Qatar has resulted in a twofold increase in email-based phishing attacks. Mainly spoofing FIFA's help desk, ticketing office, and team departments and managers. The campaigns extend to the use of malware that aims to extract confidential information and credentials in addition to device takeovers[8].

[7] https://www.grantthornton.com/insights/articles/advisory/2022/its-time-to-upgrade-cybersecurity-internal-audits.html

[8] https://www.scmagazine.com/brief/social-engineering/world-cup-raises-phishing-attacks-against-middle-east-countries

Conclusion

Grant Thornton published the "The Economic Cost of Cybercrime"[9] report which established the cost of cybercrime to be €9.6 Billion and the surge in attacks in 2021-2022 culminates in increased cyber costs for organisations. From January to July 2022, hackers stole €1.8 billion worth of cryptocurrency[10]. This accounts for a 37% increase from 2021 during the same period. These Irish and international cyber trends would indicate that the impact of cybercrime in 2022 will be in excess of €10 Billion.
While detecting and responding to attacks is still crucial for organisations in Ireland, a more structured strategic approach may be needed to prevent cybercrime.

Opportunities for improvement broadly focused on the supply chain, can be summarised three steps below:

1. Know what you have – organisations should be able to maintain updated records of their data and information assets based on their criticality ranking. Knowing what assets an organisation has, has helped estimate the effort required to secure them from a cyber breach. Extending this knowledge into the supply chain is increasingly important as this route of attack continues to impact Irish organisations.
2. Drive awareness – Cyber security awareness is critical at all levels of an organisation. Awareness campaigns and targeted training and education are great ways of engaging employees and ultimately building a cyber-aware culture.
3. Maintain consistency – Cyber security must be applied consistently throughout organisations. Security technologies, processes and independent assessments should work together to create a consistent and robust security environment.

No industry is immune from threat actors looking to steal data and hold companies hostage. Barely a day has passed in 2022 without a cybercrime or data breach being reported. The cost of data breaches is likely to keep rising as evidenced by the numerous research conducted and is anticipated in 2022 to be in excess of €10 Billion. Therefore, it is prudent to to implement measures to prevent cyber-attacks rather than respond to cyber breaches.

As the year draws to a close there is some good news. As recently as 21st November 2022, the National Cyber Security Centre (NCSC) of Ireland have made available a self-assessment tool[11] aimed at raising cyber security awareness, finding gaps in maturity of deployed controls, and assisting the plans for better cyber security maturity, resilience, and measures that will combine to reduce the risk of a cyber-attack.

[9] https://www.grantthornton.ie/insights/publications/cost-of-cyber/
[10] https://www.privacyaffairs.com/cryptocurrency-scams-2022/
[11] https://www.ncsc.gov.ie/guidance/

Contact

For more information please reach out to Grant Thornton contacts below

Mike Harris
Partner, Forensics and Cyber
T +353 (0)1 436 6503
E Mike.Harris@ie.gt.com

Howard Shortt
Director, Forensics and Cyber
T +353 (0)1 408 6948
E Howard.Shortt@ie.gt.com

Rida Villanueva
Director, Forensics and Cyber
T +353 (0)1 433 2456
E Rida.Villanueva@ie.gt.com

Offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick, Longford and Isle of Man.

grantthornton.ie @GrantThorntonIE Grant Thornton Ireland

Grant Thornton

grantthornton.ie