Grant Thornton

The Economic Cost of Cybercrime

Ireland 2021

Contents

Foreword from the Head of Cyber Security

Mike Harris
Partner,
Head of Cyber Security
Grant Thorton Ireland
T +353 (0)1 436 6503
E mike.harris@ie.gt.com

Cybercrime poses dramatically increasing risks to organisations and individuals across Ireland and the world, with daily reports of attacks taking place. It's clear that cybercriminals do not distinguish between their victims; they simply exploit whatever they can with the intent to steal funds, information or to cause disruption.

Cyber criminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the pandemic and unstable social and economic situation around the world. At the same time, the even higher dependency on connectivity and digital infrastructure due to the global lockdown increases the opportunities for cyber intrusion and attacks.

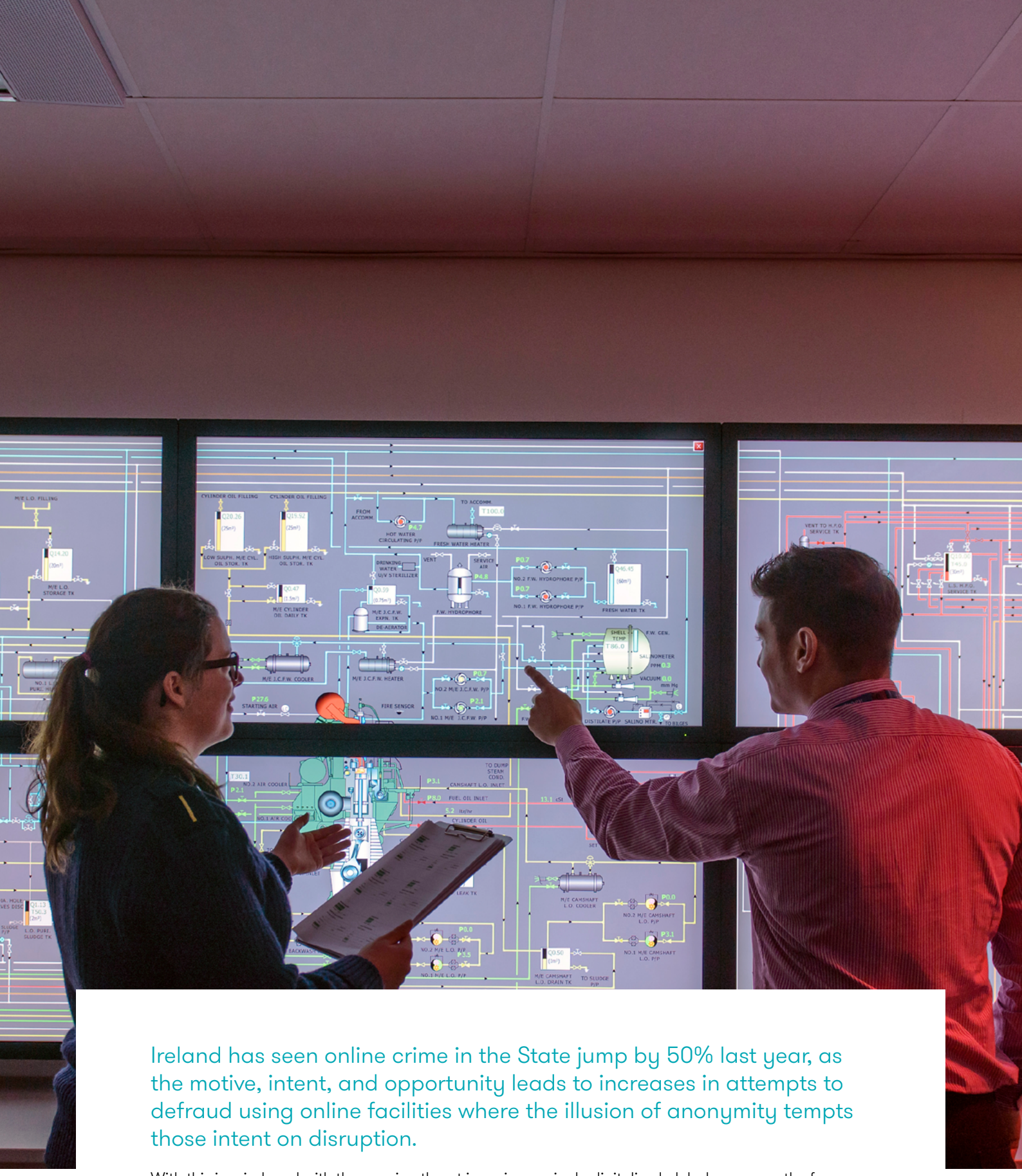
As this report shows, Irish businesses are extremely vulnerable to cybercriminals, they should be focusing their planned cyber security investments on the ability to detect and react to data-security breaches. In the current environment, it is not a question of 'if' an Irish business will be the victim of a cyber-attack but a question of 'when'. In fact, the ability of businesses to detect and react to an attack will be the key factor in limiting the impact.

As COVID-19 continues to persist globally, a further increase in cybercrime is highly likely in the near future. Attracted by the vulnerability related to working from home and the potential for increased financial benefit, cybercriminals are highly likely to build up their activities and develop increasingly advanced and sophisticated ways of operating. They are likely to continue proliferating COVID-19-themed online scams and phishing campaigns.

Business email compromise schemes will also likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activity. In addition, now that COVID-19 vaccines and medication is widely available, it is highly probable that there will be another spike in phishing related to these medical products as well as network intrusion and cyberattacks to steal data.

Even when cases of the COVID-19 decline, cybercriminals will most certainly adapt their fraud schemes to exploit the post-pandemic landscape aiming to target the largest possible number of victims.

Mike Harris
Head of Cyber Security



Ireland has seen online crime in the State jump by 50% last year, as the motive, intent, and opportunity leads to increases in attempts to defraud using online facilities where the illusion of anonymity tempts those intent on disruption.

With this in mind, and with the growing threat in an increasingly digitalised global economy, the focus of this report will centre on cybercriminals whose main objective is financial gain. Through this study we intend to put a monetary value on the economic impact of cybercrime to individuals, businesses and the Government of Ireland.

This report has been co-authored by various partners, fraud experts, and cybersecurity specialists within Grant Thornton Ireland, with the aim of providing an indication on the cost and impact of cybercrime to the Irish economy. This report also intends to provide an overview of the changing cyber trends in 2020 and an insight into the most severe forms of cybercrimes which are prominent in Ireland. The fraud risks which emerged with the onset of the global COVID-19 crisis are also explored with a focus on how organisations can minimise fraud risk by utilising the appropriate tools and techniques.

Introduction

As businesses and consumers adapted to new technologies over the past decade, so too have cybercriminals found new ways to exploit them. These cyber-attacks bring a huge financial cost to businesses, not just in the crime itself, but also in the subsequent clean-up that is required.

Seven years ago, in 2014, the first Grant Thornton Ireland report into the cost of cybercrime in Ireland revealed a total cost of €630 million to the Irish exchequer, a figure which shocked many at that time. Since then, that figure has risen dramatically with the Economic Cost of Cybercrime report from Grant Thornton Ireland revealing a total cost of €9.6 billion in 2020.

Cybercrime | *Cy • ber • crime*

refers to the use of computers to carry out crime and the term is used to encompass a range of criminal activities that use Information and Communication Technologies (ICT).

The onset of the COVID-19 crisis posed new dangers as opportunistic and coordinated cybercriminals sought new ways to exploit the novel virtual workforce that emerged internationally as employees began working from home. The sudden explosion of professionals using personal and business computers and devices to work remotely, although innovative, exposed new risks for businesses and employees. The addition of these devices into an organisation's working environment is increasing the attack surface, and cybercriminals now have extended access to target and penetrate organisation's most critical assets, data, and operational environments.

Phishing campaigns, commonly referred to as email scamming, and online fraud have emerged as some of the biggest threats impacting organisations and employees in Ireland. An Garda Síochána figures released in June 2020 revealed a 55% increase in online fraud, and phishing complaints rose by 45% during the period March 1 to May 31 2020, compared to the same time last year[1].

€9.6 billion
total economic cost of cybercrime in Ireland in 2020

55% increase in online fraud

45% rise in the number of phishing complaints

€12 million
lost to debit and credit card fraud by Irish consumers in the first half of 2020

36 billion
records compromised in 2020

334%
increase in the volume of records compromised from 2019 to 2020

1 Significant Reduction in Crime Trends during Covid-19 Pandemic – March/April/May 2020

43%
of employees face no restrictions accessing work-related documents remotely

33%
of employees use the same password for work and personal devices

30%
of employees use personal emails to share confidential work materials

20%
of employees received no training or guidance to on protecting themselves from a cyber-attack

50%
of employers have asked employees to use their personal devices for work

Significantly, there has been a 19% increase in Operational Technology (OT) attacks from 2019 to 2020[2], as cybercriminals attempt to access industrial systems. This worrying trend is likely to continue upwards.

Data breaches have also been on an upward trend in recent years prompting huge concerns for businesses around storing and protecting information. 2020 recorded the exposure of 36 billion records[3], representing 334% increase on the volume exposed in 2019 (8.3 billion).

Businesses must prioritise cybersecurity as remote working continues, and greater efforts are required by businesses to protect sensitive data as well as ensuring compliance with General Data Protection Regulation (GDPR). However Irish companies have not done enough to prevent heightened security risk in light of the widespread hybrid workforces, according to recent research by Microsoft. The study surveyed 500 employees and 200 business decision makers in September 2020 about remote working, digital security behaviour, and security concerns faced by both employees and employer.

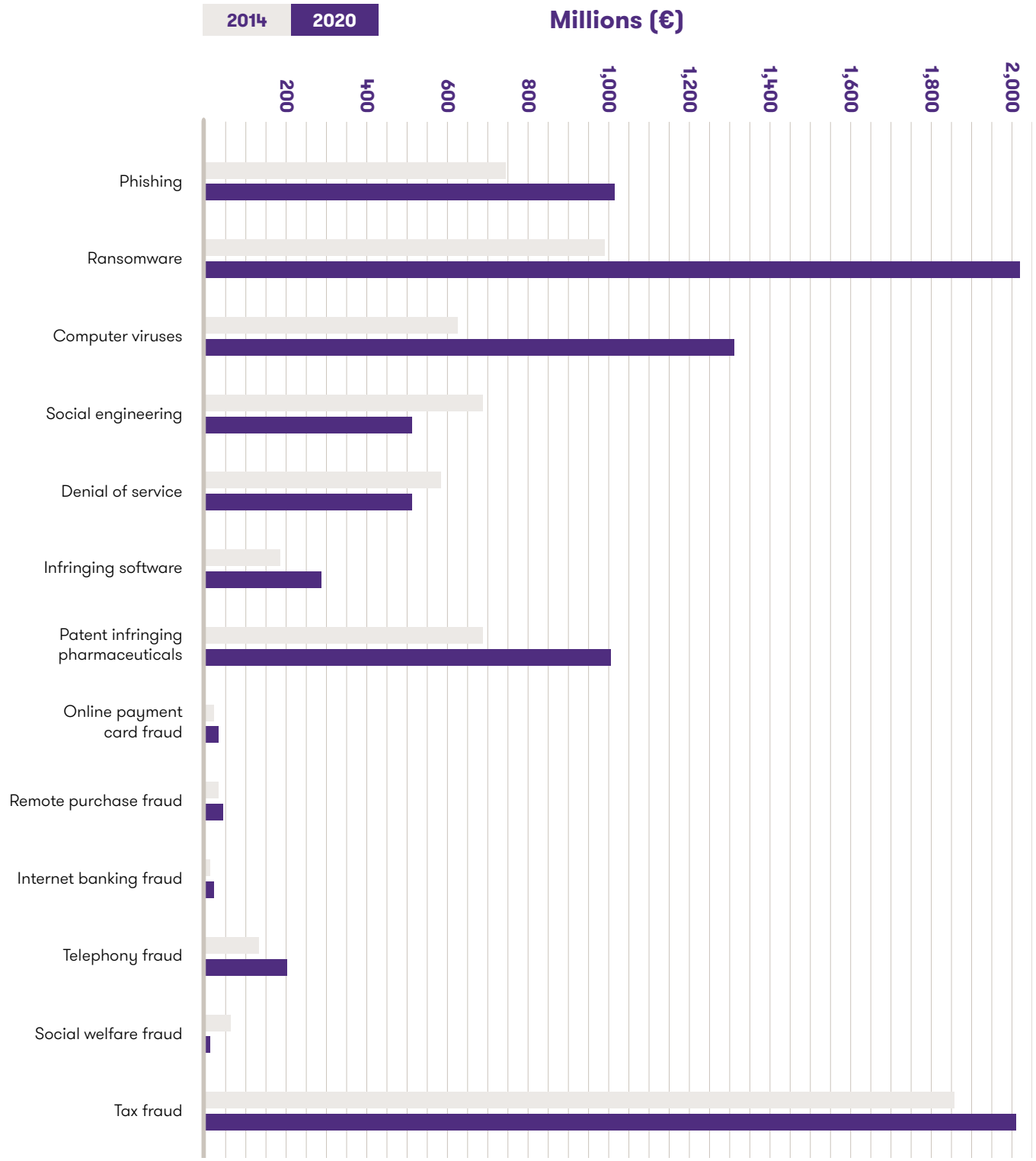
The research indicated that 43% of employees face no restrictions when accessing work-related documents remotely, Some 33% use the same password to log into work and personal devices; 30% of employees use personal emails to share confidential work materials; one in five employees have experienced a cyber-attack; and most notably, 20% have received no training or guidance on protecting themselves from a cyber-attack.

From an employer perspective, over 50% have asked their employees to use personal devices and over a third agree that their employees are taking more risks with cyber security than they did before the pandemic. However, 30% of employers will increase their security investment in 2021. From this study, it is clear that Irish companies must up their game in recognition of the growing risks associated with a hybrid workforce[4].

2 36 billion records exposed in data breaches in 2020
3 2020 State of Operational Technology and Cybersecurity Report
4 Have Irish Organisations Overlooked Security In The Race To Adapt To Remote Working?

Irish estimate figures

The graph below provides the values for each category of cybercrime as measured originally in our first report, 2014 against today's values.



Changing trends

The COVID-19 crisis and the largest economic stimulus package in Irish history have fraudsters waiting in the wings to take advantage and exploit businesses and consumers.

Paranoia and uncertainty surrounding COVID-19 is fuelling and aiding cybercriminals in their effort to dupe individuals, businesses, and government agencies. Whilst officials struggled to come up with plans and quarantine procedures, cybercriminals mobilised quickly, luring victims with the promise of new and exclusive information on protection procedures, such as COVID-19 personal protection equipment and COVID-19 therapies on dark net e-commerce sites, which studies have shown are not effective. There has been a notable increase in malware, or malicious software, being introduced to private organisations and public-sector institutions, disguised as agency-distributed guidelines.

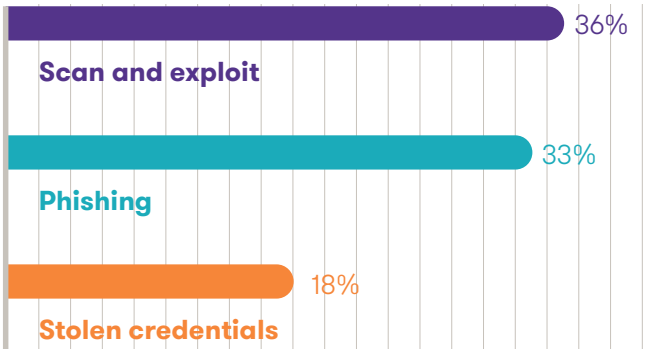
The National Cyber Security Centre (NCSC) in Ireland, and other trusted partners, have observed a significant increase in phishing and malware campaigns occurring against the backdrop of the COVID-19 pandemic. The NCSC assesses that cybercriminals will attempt to gain access through indiscriminate phishing campaigns by compromising websites or weaponising documents. These bad actors are exploiting businesses and organisations through blackmail, ransomware or payment redirection fraud. Invoice Redirection Fraud is often targeted and carefully researched and may leverage the sense of urgency created by the economic damage of the pandemic[5]. Garda figures obtained by RTÉ's Morning Ireland show €7.9 million was taken from people in online investment fraud up to the end of July 2021. That is an 86% increase when compared to the same period in 2020[6].

€7.9 million
stolen through online investment fraud in 2021

86% increase
in online investment fraud total compared to same period in 2020

5 NCSC Cyber Security Advisory COVID-19 Cyber Threat
6 Nearly €8m stolen in online investment fraud so far this year

Top initial infection vectors in 2020



Source: IBM X-Force Threat Intelligence Index 2021

A worrying figure that has emerged in the *IBM Security X-Force Threat Intelligence Index 2021* is that ransomware attacks made up 33% of all Operational Technology (OT) attacks in 2020. This suggests that malicious threat actors may be targeting OT networks as they find them more appealing. Incidents stemming from insider threats made up 13% of all OT related incidents with the majority caused by malicious insiders and the rest due to negligence in the organisation. From the research conducted by X-Force, it was observed that employees connecting to suspicious websites or selling company information on third party websites caused many of the incidents.

Another trend which has emerged was the increase in vulnerabilities in Industrial Control Systems (ICS). X-Force observed a 49% yearly increase in ICS vulnerabilities since 2020. These vulnerabilities increase the risk for operational technology systems which can have detrimental effects if compromised.

Also, the top three initial infection vectors seen in X-Force IRIS engagements in 2021 were a very close first, second, and third: scan and exploit (35%), phishing (33%) and stolen credentials (18%). Scan and Exploit, most notably, jumped up to the top infection vector in 2020, which surpasses phishing. By contrast, the credential theft decreased to 18% compared to 29% in 2019[7].

7 IBM X-Force Threat Intelligence Index 2021

Not only has cybercrime been increasing in the area of financial exploitation but cyberbullying has become a greater problem due to the major shift to digital platforms and increased usage of social media. A 2020 World Health Organisation study shows Irish teens rank in the top ten EU countries for cyberbullying experiences and unhealthy overuse of social media. This number was significantly higher for girls; 24% said they had experienced cyberbullying compared to just 12% for boys. The study focused on 227,000 schoolchildren aged 11, 13 and 15 from 44 countries across Europe[8].

The banking industry was disproportionately affected, experiencing a 1,318% year-on-year increase in ransomware attacks in the first half of 2021[9]. Ransomware was a major threat to global organisations in the first half of 2021, but it was not the only one. Trend Micro's report also reveals:

- Business Email Compromise (BEC) attacks increased by 4%, potentially as a result of new COVID-19 opportunities for threat actors.
- Cryptocurrency miners became the most detected malware, having surged ahead of WannaCry and web shells in recent months.
- The Zero Day Initiative detected 770 vulnerabilities, a slight (2%) drop from H1 2020.
- A total of 164 malicious apps related to COVID-19 scams were detected, 54% of which impersonated TikTok.

24%

of girls aged 11, 13 and 15 have experienced cyberbullying

1,318%

increase in ransomware attacks in the banking industry in 2021

Zero Day Initiative (ZDI)

refers to a bug reporting program that encourages the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers.

8 WHO 2017/2018 Health Behaviour in School-aged Children Survey
9 Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats

Most severe types of cyber events leading to cybercrime

Cybercrime can be divided into subcategories based on whether they are traditional crimes that now take place online; transitional crimes whose pattern has changed as a result of moving online; new or genuine crimes which are only in existence thanks to the internet, and finally, platform crimes which facilitate crimes as opposed to executing the crime itself.

Cyberwarfare

This involves the actions by a nation-state or international organisation to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

The Stuxnet worm was one of the world's first instances of weaponised computer code utilised during cyberwarfare. Stuxnet was most famously used against a nuclear research facility in Tehran in 2012.

The worm exploited four zero-day flaws within the research facility's system, infecting over 60,000 state-owned computers, and physically destroying approximately 1,000 nuclear centrifuges. This was around a fifth of the total owned by Iran and slowed nuclear projects by a number of years.

Destructive malware attacks

Short for malicious software, it takes the form of hostile or intrusive software, including computer viruses, ransomware, spyware, and scareware (social engineering). Most destructive malware variants cause destruction through the deletion or overwriting of files that are critical to the operating system's ability to run. In some cases, destructive malware may send tailored messages to industrial equipment to cause malfunction.

Invoice-redirect fraud

This involves crime gangs tricking companies into lodging money into accounts controlled by the criminals. They send invoices to companies purporting to come from one of the targeted companies' trading partners.

Denial-of-Service (DoS)

This type of attack shuts down a network by flooding the target with traffic, or sending it information that triggers a crash, making it inaccessible to its intended users. Such attacks are a very common technique used by cyber crooks to distract bank officials when carrying out a money heist.

Ransomware

This is a type of malware which threatens to leak private and confidential data. The fear is enough for a victim to pay the ransom that is demanded by the cybercriminal. Destructive malware activity shows that this potentially catastrophic malware trend continues to be a rising threat.

Why estimate the cost of cybercrime?

The growing volume of cyber-attacks being carried out point to an urgent need to safeguard data more than ever. Understanding the landscape of cybercrime is pertinent to preventing these attacks from being successful.

This urgency is evident as 59%[10] of the world's population now has access to the internet as of October 2020, and household internet access increased to 93% in March 2020, an increase from 91% in 2019[11]. When attacks occur, criminals often leave little or no trace of their presence. As more aspects of our lives become dependent on the internet, more criminals will emerge to stake their claim.

Despite recent developments in this area, some believe that cybercrime is not a major concern and that the chances of a cyber-attack happening to a person or business are slight. The reason for this misconception is the severe underreporting of cybercrime which acts as a strict barrier to our understanding of its true scale and cost. There are three main reasons for the underreporting of cybercrime:

- the fear of reputational damage;
- the victim not knowing whom to report the attack to; and
- the victim is often unaware that an attack has taken place.

Preparing for a cyber-attack is an extremely difficult task when many business owners and individuals are unaware of, or underestimate, the losses that they could incur. For maximum protection, companies ideally would not only make themselves an unfavourable target to cybercriminals but also implement security mechanisms to; know what assets are connected to the network, the importance of those assets, the implementation of and measurement of, control effectiveness. Companies should have an incident response plan. If you run a business, whether big or small, the question is not if a cyber-attack will happen, but instead when it will happen or if it has already occurred.

In a survey of 1,000 business leaders carried out by the Institute of Directors (IOD), some 95% of respondents considered cyber security to be very important. A much lower 55% of them, however, have a formal cyber security strategy set in place and only 44% have employee cyber awareness training. Although they recognise the threat posed by inadequate cyber security, just over half are taking steps to prevent and mitigate against that risk.

While **95%**
consider cyber security to be very important;

only **55%**
have a formal cyber security strategy; and

only **45%**
have cyber awareness training for employees.

Source: Institute of Directors Survey 2020

10 Global digital population as of January 2021
11 Impact of COVID-19 on ICT Usage by Households

The database compromises of 2021 have confirmed yet again, that breaches are the third certainty in life, and we are all living in a constant state of cyber insecurity.

Responding to cybercrime is a business decision. In making that decision, businesses must weigh the level of risk they are willing to accept and its potential costs and implications, against the investment required to manage and reduce that risk. Citizens are just as much at risk as businesses are and need to assess their own risk profile.

Cost to the government

As illustrated in the *National Cyber Security Strategy 2019-2024*, the Irish Government acknowledges that cybercrime is a growing phenomenon. They recognise that it must be taken seriously, however, no actual figures are given to indicate how much of the defence budget will be allocated to cyber.

Ireland's first National Cyber Security Strategy was agreed by Government and published in July 2015. It set out a road map for the development of the National Cyber Security Centre (NCSC) and a series of measures to better protect government data and networks, and critical national infrastructure. This period since that time has seen the NCSC grow significantly in scale and capacity, as well as the introduction of the EU Network and Information Security Directive 2016/1148 (NIS Directive), a significant set of measures to support government departments and agencies in managing their systems.

The Irish Government announced in February 2021 that it is investing €193 million over six years into research on cybersecurity, artificial intelligence, ethics, and data privacy, and smart medical devices[12]. It is a reflection of a growing concern among nation states of the vulnerabilities which emerge when evolving and new technologies are relied upon across large sectors of society.

One such example is the emergence of Fifth Generation (5G) networks. Ensuring resilience of 5G networks is essential to our society as this technology is expected not only to have an impact on digital communications, but also on critical sectors such as energy, transport, banking and health, as well as on industrial control systems. 5G networks will be carrying sensitive information and will be supporting safety systems that will come to rely on them[13].

Fifth Generation (5G)

refers to the next generation of mobile internet connection and offers much faster data download and upload speeds. Through greater use of the radio spectrum it will allow far more devices to access the mobile internet at the same time.

Member States, with the support of the Commission and the European Agency for Cybersecurity published a report on the EU coordinated risk assessment on cybersecurity in 5G networks. This major step is part of the implementation of the European Commission Recommendation adopted in March 2019 to ensure a high level of cybersecurity of 5G networks across the EU.

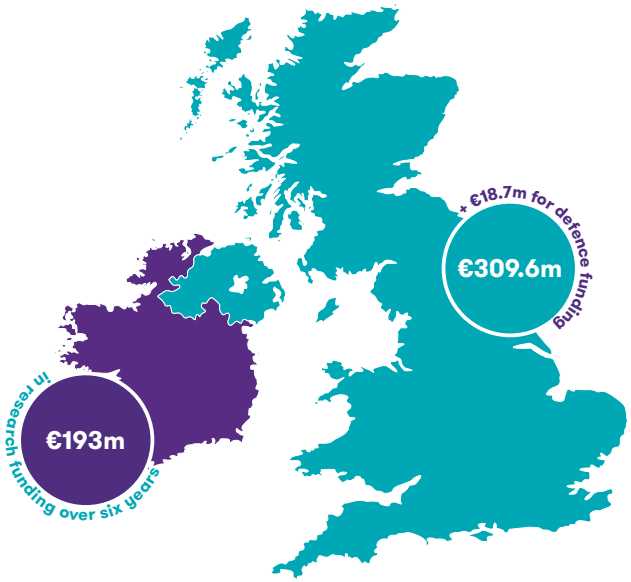
The report sets out the main types of threats posed by 5G networks, and specifically, how threats posed by states or state-backed actors, are perceived to be of highest relevance. The combination of motivation, intent and a high-level capability enables states to perpetrate attacks that can be very complex and have a major impact on essential services for the general public, deteriorating the trust in mobile technologies and operators.

12 Minister Harris announces €193 million investment in five world- leading SFI Research Centres
13 Report on the EU 5G Toolbox Implementation by Member States Published

For example, states or state-backed actors can cause large-scale outage or significant disturbance of telecommunications services by exploiting undocumented functions or attacking interdependent critical infrastructures (e.g. power supply). The report also assessed the main vulnerabilities, which includes supplier specific vulnerabilities. The increased role of software and services provided by third party suppliers in 5G networks leads to a greater exposure to a number of vulnerabilities that may derive from the risk profile of individual suppliers[14].

Across the Irish sea, the UK Government gave a figure of up to £265 million to go towards defence of their military cyber systems. This equates to €309.6 million*. Although it is specifically military based, it is nonetheless a small fraction of the actual cost of cybercrime in Ireland which is calculated at 22 times that figure (€9.6 billion). Additionally, as of November 2020, the UK Government announced a €18.7 million* rise in defence funding with the extra money being used to modernise the armed forces with more spent on robots, autonomous systems and meeting new threats in the domains of space and cyber[15].

Recent figures for Irish and UK government spending on cyber security



*The converted rate is based upon interbank rates as of 11:30am 11 November 2021.

Conversion rates
£1 = €1.1684
$1 = €0.8724

14 Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures
15 Defence funding boost 'extends British influence', says PM
16 Technology Ireland, Future Needs Future Thinking 2021

The workplace upheaval caused by COVID-19 resulted in a rise in attempted and successful cybercrime, highlighting the need for urgency in rolling out the National Cyber Security Strategy.

Government must ensure that our national cyber security and data protection capabilities are adequately resourced, and that Ireland is seen internationally to be playing a strong role in protecting critical infrastructure and managing cyber risks[16].

Furthermore, 5G infrastructure is the future backbone of our increasingly digitised economy and society. Billions of connected objects and systems are part of this network, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Ensuring the security and resilience of 5G networks is therefore essential. Government must ensure that they introduce security measures to cover all areas identified by the EU in its report on the EU coordinated risk assessment on cyber security in 5G networks, in order to protect the next generation of mobile networks from cyber-attacks.

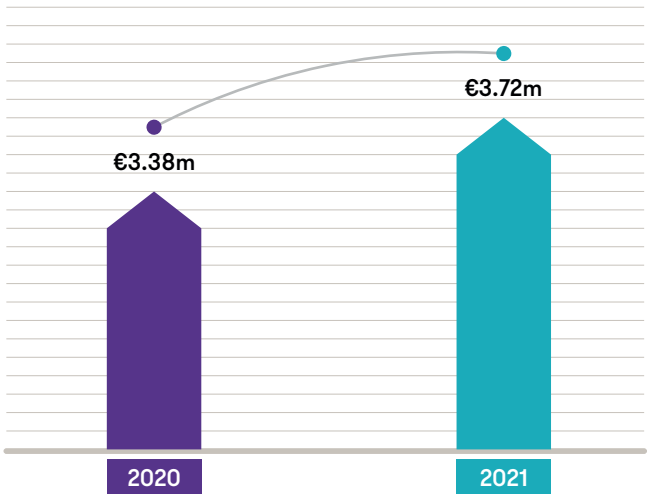
Cost to businesses

A value must also be put on the customer base that is lost by a business following a data breach.

According to the *IBM Cost of Data Breach Report 2021*, in order to calculate the cost of a data breach, a value must be assigned to lost business which includes the activities that attempt to minimise the loss of customers, business disruption and revenue losses. Reputational losses and diminished goodwill must also be factored into this. The IBM report used an accounting method called activity based costing, which identified activities and assigned a cost according to actual use. Four process-related activities drive a range of expenditures associated with an organisation's data breach: detection and escalation, notification, post data breach response and lost business.

The IBM global study indicated data breach costs rose from €3.38 million* to €3.72 million*[17], the highest average total cost in the 17-year history of this report. The average cost was €950,000 higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor.

Data breach costs



Source: IBM Cost of Data Breach Report 2021

Despite an increased level of awareness, cybercrime incidents in Ireland are increasing with 61% of Irish organisations reported to have fallen victim to cybercrime such as fraud in the last two years, with an estimated loss on average of €3.1m

National Cyber Security Strategy 2019–2024[18]

*The converted rate is based upon interbank rates as of 11:30am 11 November 2021.

Conversion rates
£1 = €1.1684
$1 = €0.8724

17 IBM Cost of a Data Breach Report 2021
18 Cybercrime: Current Threats and Responses

A recent global report by Hiscox Insurance[19], which included more than 300 Irish companies surveyed in Ireland, has found that 43% of Irish firms had experienced at least one cyber attack. The hackers' favourite targets were the Technology, Media and Telecoms (TMT), financial services and energy sectors.

One-in-six of all firms attacked this year (17%) said the impact was serious enough to 'materially threaten the solvency or viability of the company'. With ransomware now commonplace, around one-in-six of those attacked was hit with a ransom and more than half (58%) paid up. Successful attacks for ransomware stemmed from phishing attacks in 65% of reported incidents. Irish firms (from a pool size of 20) reported 75% had paid a ransom.

Interestingly, the first point of entry for a cyber-attack is reported with 37% being a corporate-owned server, 31% a corporate cloud server, and importantly, 23% being employee-owned mobile devices.

A key finding in the report highlighted that Irish firms were joint third of eight countries measured for spending on cyber security in enhancing disaster recovery capabilities, improving the security of customer-facing services and apps, and enhancing top management engagement in cyber policies and procedures. Disappointingly Ireland also had the largest proportion of firms (36%) ranked as cyber novices. Luckily however, Irish firms suffered median costs of just €7,251* in comparison to a median of €8,736* to €103,000* at the 95th percentile for those organisations employing between 50 and 249 employees. Larger organisations suffered a proportionally higher cost of €21,000* at median to €404,000* at the 95th percentile.

Financial services are among the most attractive targets for cyber-attackers as criminals steal sensitive data that can be used to open fake accounts and lines of credit they need for success[20].

43%
of irish companies had experienced at least one cyber-attack

Source: Hiscox Cyber Readiness Report 2021

Financial services

Most attractive targets for cyber-attackers

19 Hiscox Insurance Cyber Readiness Report 2021
20 Financial services top cyber attack target

Irish businesses should take steps now to secure their environment.

As a first step, businesses should establish an awareness and training program to help educate employees on their responsibility to help protect the confidentiality, availability and integrity of their organisation's information and information assets. This training should also engage the workforce on security implications of working from home and cover key remote work leading practices (e.g. sharing files securely, using VPN, maintaining secure passwords, ensuring security of wireless and home network configurations, adapting to shared living environments, and securing physical company-owned IT assets).

Additionally, Irish businesses should improve their threat detection and response capabilities to detect and respond to ransomware attacks, revisit security monitoring controls, update incident response and crises plans, and enhance security architecture in high risk areas.

Cost to individuals

Consumers are as vulnerable to cyber-attacks as businesses are, which is evident in the rise of online phishing scams in recent years. However, measuring the total cost of cybercrime on individuals is difficult due to the various indirect costs incurred.

According to figures published by the Banking and Payments Federation Ireland (BPF) in April 2021, Irish consumers lost over €12m through debit and credit card fraud in the first half of 2020[21].

While a victim of card fraud can measure exactly what was stolen from their accounts, the cost of changing card details and rectifying damages must also be taken into account. The time involved in reconciling losses and damages also comes with a cost as it reduces time available to allocate to other tasks. Again, however, this is difficult to measure.

Formjacking | *Form • jack • ing*

the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of ecommerce sites.

Incidents of formjacking trended upwards in 2018.

Formjacking credit cards has become so popular that the average price for a credit card sold on the black market is €40*, which means that just 10 credit cards stolen from 4,818 compromised websites could result in a yield of up to €1.92 million* for cybercriminals each month[22].

This has become more prevalent during the COVID-19 pandemic as more and more people are shopping online. Even when cases of the COVID-19 have declined, cybercriminals will most certainly adapt their fraud schemes to exploit the post-pandemic situation and the largest possible number of victims.

€40/ 

× 4,818 compromised websites

€1.92 million

potential monthly yield for cyber criminals

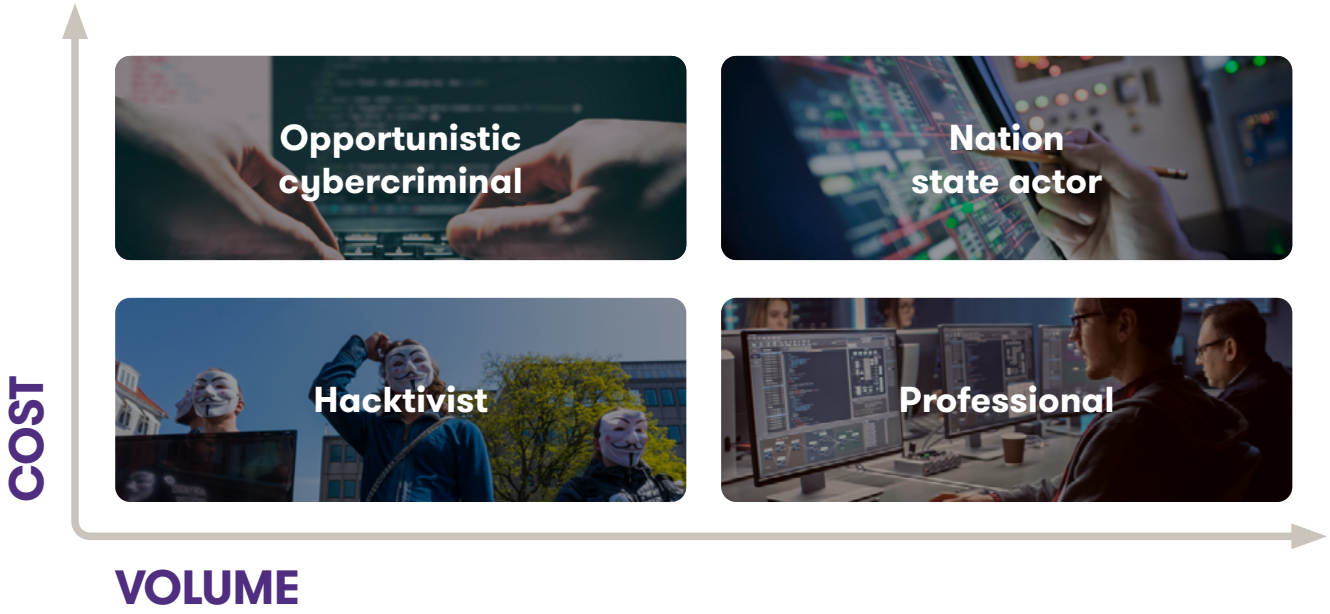
*The converted rate is based upon interbank rates as of 11:30am 11 November 2021.

Conversion rates
£1 = €1.1684
$1 = €0.8724

21 Shoppers hit with over €12m in debit and credit card fraud in first half of 2020
22 Symantec 2019 Internet Security Threat Report

Who are the criminals and who do they target?

Anyone engaging in computer-based crimes is categorised as a cybercriminal, they are further characterised based on what they aim to achieve and whom they target.



Although financial gain is the key factor as to why most individuals and groups participate in cybercrime, there are some who do so for ideological reasons. So called **hacktivists** for example, use the internet to promote their religion, politics and/or cause and engage in the hacking of computer networks as a form of protest.

Opportunistic cybercriminals are the next step up from hacktivists. Although they do strive for some financial gain, they are small scale in what they take and whom they target, commonly targeting individuals and smaller, vulnerable targets. Their focus involves targeting large numbers for small values.

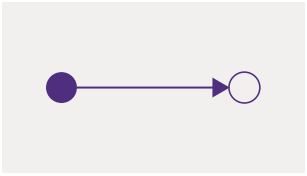
The next step up from opportunistic cybercriminals are **professional criminals** who run large, organised crime networks. Cybercrime is attractive to criminals as the rewards are high and the risks are low. This type of crime varies in severity from online theft to industrial espionage. Targets typically include big businesses in the financial and health sectors as these have an abundance of sensitive personal information that is worth a lot of money.

The most sophisticated of cybercriminals, however, are the **nation-state actors**. These are highly organised individuals/groups with considerable and sophisticated techniques and resources. They specialise in the deliberate attack of information systems for military, or political purposes either through the theft of IP or business confidential information.

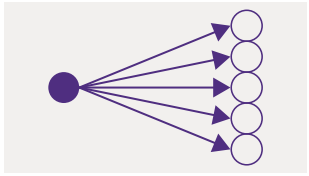
Occasionally, cybercrimes are carried out by legitimate organisations whose motive is to acquire IP and company-sensitive data from rival companies to gain the upper hand in innovations or the market. This is called **cyber espionage**.

Another important point to note is that cybercriminals can work alone or work together. When targeting individual citizens typically they work alone, targeting one or several citizens through identity fraud etc. If they choose to work together it could mean that more is to be gained from their targets, like large successful businesses or financial services. They can work together to attack an individual target or they could collectively attack several. An illustration of this can be seen below[23].

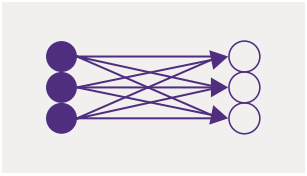
One-to-one attack



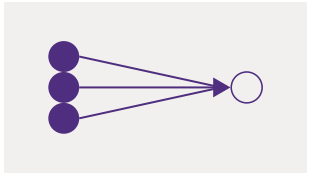
One-to-many attack



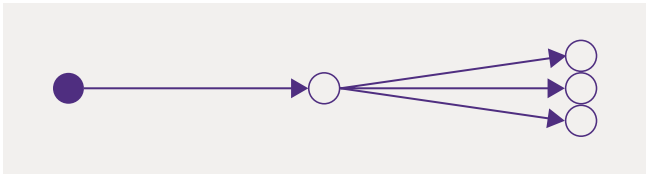
Many-to-many attack



Many-to-one attack



Multi-stage hybrid attack



Source: Mark Johnson, Cybercrime, Security and Digital Intelligence (2013)

Anyone with access to the internet is at risk of a cyber-attack. It does not matter if you are a citizen, work in a business or for a government.

As financial gain is the primary motive, cybercriminals target businesses which they believe to have the most valuable information such as personal data – name; Personal Public Service Number (PPSN); date and/or place of birth - and intellectual property and business confidential information.

Investigating the cost of cybercrime gets complicated when we try to place a definitive value on it. Though it is a difficult task, it is not impossible. To help put things into perspective, *IBM's 2020 Cost of a Data Breach Report*, provides figures on the cost of a data breach broken down into the price for which a single confidential or personal document would sell.

Compromised record

refers to information that identifies a person whose information has been lost or stolen in a data breach attack.

The average price for which a compromised record containing sensitive and confidential data such as customer Personal Identifiable Information (PII) would sell is €130*[24]. At first glance this seems like a relatively low number, but a single data breach could result in tens of thousands of records stolen. This is on a large scale, however, and some cybercriminals instead target individuals. As they do not obtain the same amount from one individual as they would one business, they target numerous individuals to compensate for any less-valuable data they retrieve during cyber-attacks.

*The converted rate is based upon interbank rates as of 11:30am 11 November 2021.

Conversion rates
£1 = €1.1684
$1 = €0.8724

23 Mark Johnson, Cybercrime, Security and Digital Intelligence (2013)
24 IBM Cost of a Data Breach Report 2020

Impact of cybercrime

Cybercrime affects everyone, through a combination of direct costs, indirect costs, and defence costs. All three factors must be considered when attempting to cost the overall economic impact that cybercrime has on citizens, businesses and a government.

Direct costs
This is the immediate, quantifiable cost of these harmful attacks. It is the monetary cost placed on the losses and damages inflicted upon the victim of a cyber-attack. Examples include money stolen directly from accounts and opportunity cost in terms of the time and effort put into restoring order after an attack, which otherwise could have been used more valuably.

Indirect costs
This is the monetary value of the opportunity costs inflicted not only on individuals but also on society, including indirect losses such as reputational damage i.e. the loss of trust in a bank that has suffered a data breach which in turn may result in customers switching to another bank; missed business opportunities that will never be realised; or the revenue lost as a result of stolen IP rendering an idea useless.

Defence costs
The monetary cost of both prevention and reaction efforts to cyber-attacks. Examples include: antivirus, spam filters, training and awareness measures for employees, fraud detection and tracking and recuperation efforts.

Cost to society
The cost to society is the sum of direct costs, indirect costs, and defence costs.

Impact on individuals

Cybercrime can have an enormous impact on its victims. Individuals might find themselves a victim of cybercrime either directly through online scams, scareware, and identity theft, or indirectly through an attack on a company that they have an association with (i.e. they are a customer).

Cyber-attacks carried out against businesses also have an indirect impact on individuals as well, but this is not one that we can reliably place a value on. The impact of cybercrime on individuals is not easy to accurately quantify and the value can vary depending on the amount of distress caused and the time and effort taken to rectify, for example, account details.

For instance, a data breach on a bank will impact an individual differently than a data breach would on a hospital. If a company has a data breach and their customers' personal and confidential information is stolen, this has an effect on each and every one of their customers. A customer whose personal information was not stolen and 'only' put at risk is still impacted as they may now lose confidence in that company and decide to move their business.

Since the onset of COVID-19, there has been a significant increase in cybercrime targeted at individuals, businesses and government agencies. To better understand consumer sentiment around data security amid the pandemic, PCI Pal, the global provider of secure payment solutions, recently conducted a survey of North American consumers.

The research found that a staggering 64% of Americans and 68% of Canadians would avoid buying from a company that had suffered a COVID-19 related data breach for up to several years. A further 17% of Americans and 24% of Canadians said they would never return to the business[25]. Human error can be vital in the success of various cybercrime incidents. Through the use of phishing emails, vishing and an assortment of other social engineering practices, individuals may be manipulated into giving away sensitive information to what they thought was a legitimate entity. Similarly, an individual may believe a fake advertisement and lose money on a product that is never delivered or a product that does not reach the standard or quality that was promised.

Vishing | *Vish • ing*

The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

25 New North American Consumer Research by PCI Pal Shows Significant Financial Consequences for Businesses That Suffer COVID-19 Related Data Breaches

Impact on businesses

Utilising IT and experiencing the benefits of having a web presence can significantly enhance economic profit for businesses. Equally, however, it leaves businesses open to the threat of a cyber-attack.

The risk of attack is difficult to accurately gauge and many companies struggle to balance this risk, its impacts and potential costs against the cost of defence. In terms of monetary value, the potential financial loss, as a result of a cyber-attack, could be less than the actual cybersecurity investment costs in the event of an attack occurring. But when the potential financial loss is added together with:

- the value of IP that could be stolen;
- the cost of customers lost due to the loss of confidence in the company;
- potential extortion in the form of ransomware; and
- industrial espionage which could render new ideas and inventions potentially worthless;

the overall value may be far higher than that initial investment on cyber security, as what can be more damaging than the direct monetary loss, is the cost of externalities such as the media coverage of a cyber-attack that results in the loss of current and future customers.

In other words, 'the knock-on effect' of a data breach can be devastating for a company. Getting hit with a fine is one thing, but when customers start taking their business – and their money – elsewhere, that can be a real body blow[26].

The problem with these indirect losses is that they are hard to accurately quantify and companies have a tendency to underestimate the risk, and so do not prepare adequately for a cyber-attack.

According to a study conducted by Esme Learning Solutions which surveyed over 750 business leaders released in June 2020, while **75%** see cyber security as a central priority for their organisation, only **26%** have a dedicated team and a robust cyber security plan[27].

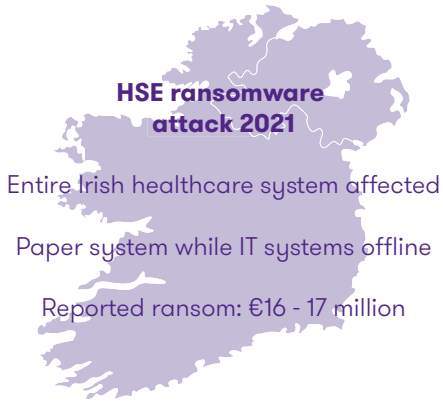
26 ICO's access to information strategy calls for better compliance by public authorities backed up with enforcement action
27 Good Cyber Security Starts in The Boardroom

Impact on government

Before the digital age there was little need to plan or budget for cybersecurity. Now, governments must take steps to ensure their nation's citizens and critical national infrastructures are safe from cyber threats. Ireland now ranks among the leading EU Member States in terms of the uptake and use of digital technologies.

The **National Cyber Security Strategy 2019 - 2024**[28] sets out a series of measures to better protect government data and networks, and critical national infrastructure. Furthermore, approximately 70 critical national infrastructure operators have been legally designated as such and have been made subject to binding security requirements and to a binding incident notification requirement. Together, these mean that the State and critical national infrastructure operators are better prepared to deal with cyber security related risks than before. The government will, over the period 2019 - 2024, implement a total of 20 initiatives and measures to protect the nation, to develop the cyber security sector, and to deepen international engagement on the future of the internet.

Disruption to systems used by Irish citizens and businesses can pose a direct threat to the functioning of the State and the economy, along with the daily lives of millions of citizens. One cyber-attack can inconvenience not only the intended target, but also those associated with them, causing many layers of complexity in the clean-up and cost of the incident. An attack on an online business can affect that business directly in terms of monetary losses, while the attack affects its customers by inconveniencing their online experience while the site is down. On a larger scale, a cyber-attack on a healthcare system can have a devastating impact on thousands of workers and citizens and is a very serious issue for government and state agencies.



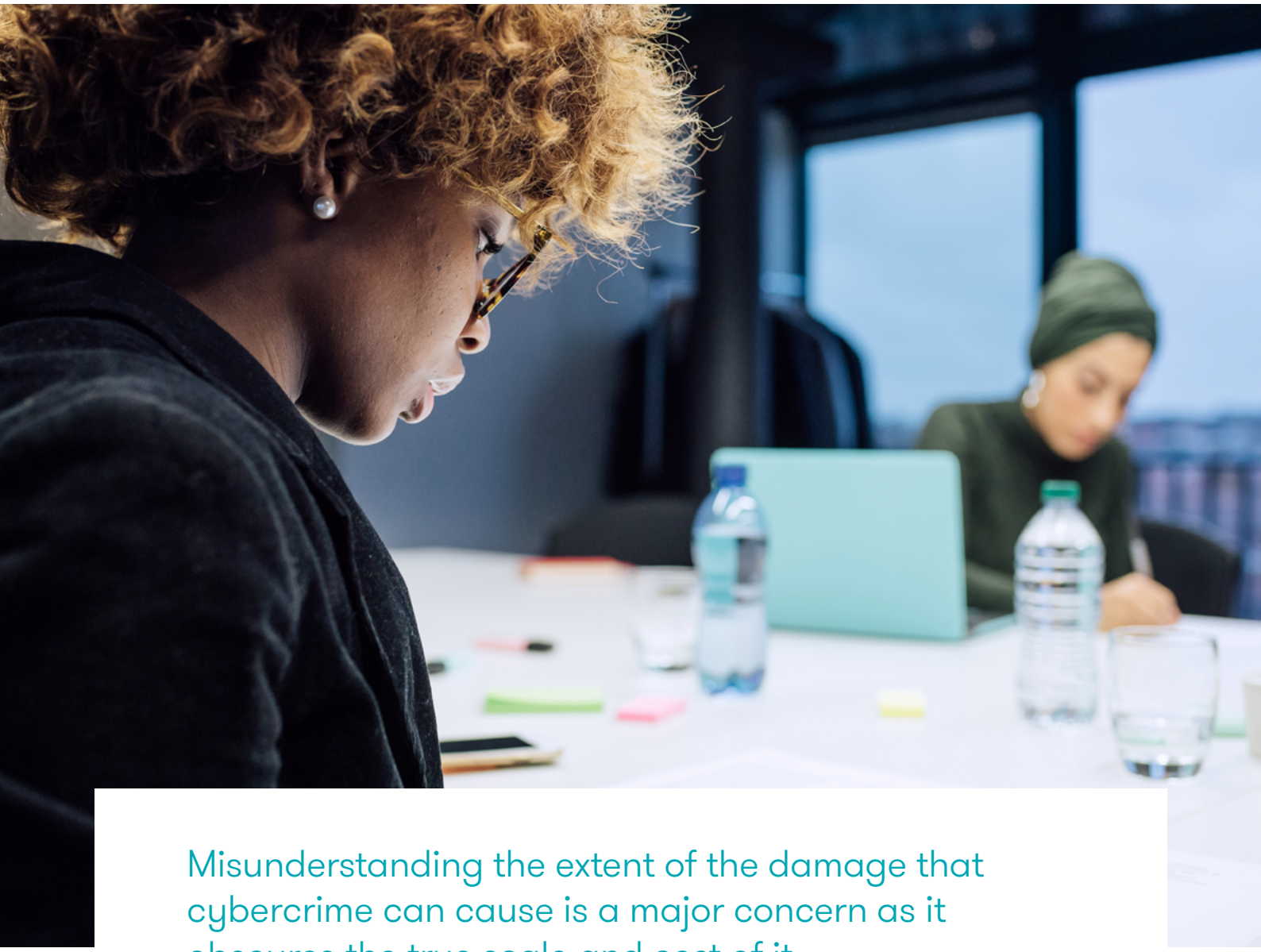
More recently, there was a large scale cyber attack against the HSE in Ireland. This cyber attack affected almost every part of the Irish healthcare system and resulted in medical staff having to use a paper system while IT equipment was offline. The ransomware group, Conti Ransomware, reportedly asked for a payment in the range of €16 - 17 million for the decryption key[29]. This attack further emphasized the requirement for effective cyber security in organisations.

*The converted rate is based upon interbank rates as of 11:30am 11 November 2021.

Conversion rates
£1 = €1.1684
$1 = €0.8724

28 National Cyber Security Strategy 2019-2024
29 HSE cyber-attack: Irish health service still recovering months after hack

Constraints and assumptions



Misunderstanding the extent of the damage that cybercrime can cause is a major concern as it obscures the true scale and cost of it.

This misunderstanding of the extent of the true cost is just one of many reasons for underreporting. Other main reasons are:

- fear of financial and reputational damage;
- not knowing to whom to report the crime;
- companies or individuals not knowing that an attack took place.

Valuing the cost of cybercrime is all the more difficult as we do not have the true picture of the number of attacks or any confirmed information on them. As a consequence, much of our work is based on estimations.

Fines under GDPR

The General Data Protection Regulation (GDPR) came into effect on the 25 May 2018 and replaced the existing data protection structure under the EU Data Protection Directive. Its aim is to ensure transparency, security and accountability by data controllers and processors, while also strengthening and unifying the right of individual citizens of Europe to data privacy[30].

Previously, the Office of Data Protection Commissioner (ODPC) in Ireland and the Information Commissioner's Office (ICO) in the UK had the powers to issue fines in relation to data protection breaches in Ireland and the UK respectively. In the Republic of Ireland, the ODPC had a maximum potential fine of €100,000 and the ICO of €584,000*. Now under the new GDPR, the maximum fine has increased to €20 million, or 4% of the organisation's turnover in serious cases. This new regulation has undoubtedly resulted in companies spending more money on their cyber security in order to prevent attacks.

Tusla, Ireland's child and family agency, was the first organisation fined under the GDPR in Ireland when subject to a €75,000 fine from the ODPC in May 2020. Twitter was issued with a fine of €450,000 for failing to promptly declare and properly document a data breach. More recently, the ODPC issued Whatsapp with a fine of €225 million for failings of transparency under Europe's GDPR. This was the ODPC's largest fine issued and is a considerable increase when compared to the previous maximum fine of €450,000 issued to Twitter.

€225 million

New maximum fine issued by the ODPC for Whatsapp's failings of transparency

Outside of Ireland, on 21 January 2019, the French National Commission on Informatics and Liberty, issued a fine to Google of €50 million. More recently, Amazon were fined €746 million by the French data protection commission (Commission Nationale de l'infomatique et des Libertes). This is the biggest GDPR fine to this date, issued for violations onthe account of lack of transparency on how the data was being harvested from users and used for ad targeting.

In order to shed some further light on the size of the GDPR fines that companies may face in the future when compared to the obsolete data protection structure, we have used real examples of previous fines issued to give an accurate picture.

For example, prior to GDPR, a private investigator was fined €4000 for the unauthorised access of data. This amount is only 4% of the maximum figure of €100,000. When compared with the new maximum fines of GDPR of €20 million, that 4% that he was fined would equate to €800,000. Although that fine would still amount to 4%, it is a huge increase.

The fine issued to Yourtel Limited in Ireland in 2017 is another telling example of the cost to businesses under GDPR. Yourtel Limited was fined €5000 for making a number of unsolicited calls to elderly Irish customers. Although only 5% of the maximum fine, when applying this percentage to GDPR this would now be equal to €1 million. With fines potentially reaching such heights, companies everywhere have been encouraged to follow GDPR very strictly, to avoid such monetary losses.

30 Data Protection Commissioner, General Data Protection Regulation
*The converted rate is based upon interbank rates as of 11:30am 11 November 2021. £1 = €1.1684

To conclude, the GDPR was simply the latest in a series of data protection legislation aimed at improving individuals' rights over their personal data and imposing penalties on organisations which fail to protect that data.

Organisations are now required to have in place systems and processes which secure the personal data held and protect the privacy of the individuals involved, which puts even more pressure on businesses to protect against cybercrime. The consequences of failure in terms of potential fines and reputational damage are potentially enormous.

Appendices

Methodology and formula

*We leveraged the methodology from the 2014 Cost of Cybercrime Report, which was previously published by Grant Thornton. As highlighted, estimating the cost of cybercrime in Ireland for 2020 is challenging, hence we collated available figures for many types of cybercrimes for each year between 2014 and 2020 and calculated the average year on year % increase to calculate the approximate 2020 figures. In other cases, where new figures became available these were utilised. These new figures were not available in 2014 when the original estimate was made. This in some cases, makes the direct comparison with individual figures the original report difficult.

It should also be noted that, a number of the figures that were collected are of global and UK origin. To have these figures approximate the Irish economy they have been adjusted in relation to Ireland's ranking of global GDP of the year 2020. This was 0.48% for Ireland while the UK was 3.15%. To calculate the Irish estimate, the UK percent of global GDP was divided by the Irish percent of global GDP to get the Irish fraction of the UK, and then the original figure was divided by this for the Irish estimate. Finally, the figure was converted from British Pounds to Euro. In the case of a global amount, the original figure is simply multiplied by 0.48% and then converted to Euro.

Assumptions for the 2020 figures and calculations:

1. **After collating some of the 2018 figures from sources for certain types of cybercrime, we calculated the % increase from the original 2014 figures to 2018 figures. Accordingly, we assumed the linear increase continued from 2018 to 2020 which allowed us to scale the figures upwards by the % increase (from 2014 to 2018) to calculate the approx. 2020 figures.

2. ***Finding data for the cost of certain types of cybercrime was not possible for any year beyond 2014. In these cases, we calculated the 2020 figures by taking the average % increase across each of the cybercrimes applicable to point 1 above from 2014 to 2018, which was an average of 215% increase. Accordingly, we applied a 215% increase from 2014 to calculate the approx. 2018 and 2020 figures.

$$\{ X/Y = P \rightarrow Q/P = E \rightarrow E\ (CC)\} = FE$$

The formula for estimating Irish figures, where:
X = GDP % of the country where the figure originated from;
Y = Irish GDP % of world GDP;
P = Irish GDP in proportion to the original countries GDP;
Q = Original figure;
E = Estimate before currency conversion (CC); and
FE = Final estimate figure after currency conversion.

When 'X', the GDP of the source date, is divided by 'Y', the Irish GDP, this gives us 'P', the proportion of Irish GDP in relation to the GDP of the source data. This then is divided into 'Q', the original source figure to give us 'E', the estimate figure. The final, crucial step is to convert 'E' into the currency used in Ireland, the Euro, to give us 'FE', the final estimation figure.

Types of cybercrime

Irish society has been fundamentally transformed by digitalisation and this has changed the way society and economy operate.

Our society is now entirely dependent on Information and Communication Technology (ICT) which has benefited us greatly but has also brought about threats and vulnerabilities that challenge cybersecurity and thus, overall stability. With this modernisation comes the opportunity for individuals and groups to exploit vulnerabilities in this new digital world.

Cybercriminals have extended beyond the confines of traditional ICT systems and functions, such as through their access to sensitive data and in their conduct of decentralised activities which may be critical in their own right. As such, digitalisation knows no personal, functional, organisational and even national bounds, creating in effect new challenges including those of privacy and security. Set out below are types of cyber-events which can lead to cyber-enabled crime:

Phishing

An act of deception where there is an attempt to pose as a legitimate and trustworthy entity, through email, websites, phone calls, Instant Messages (IMs) or social networking, in order to gain sensitive information such as usernames, passwords and/or credit card details. The underlying goal at the end of the scheme is to obtain money.

Malware

Short for malicious software, it takes the form of hostile or intrusive software, including computer viruses, ransomware, spyware, and scareware (social engineering). Malware still remains the most frequent attack method in most countries and is the costliest to resolve. Malware is now being aimed at smartphones and tablets at ever increasing rate.

Ransomware

This is a type of malware in which, through Denial of Service (DoS)[31] or the threat of leaking private and confidential data, the fear is enough for a victim to pay the ransom that is demanded by the cybercriminal.

Computer virus

Also a type of malware. A virus is usually attached to a programme, without the owner's knowledge and remains dormant until activated to execute its code. This activated code may corrupt a whole system or destroy vital data, and spread from device to device.

Social engineering

Manipulation, used to trick individuals into giving out confidential, private and/or sensitive information that will then be used for fraudulent activities. There are different ways that this can be done, either through the use of fear or a deal that appears to be too good to be true but for a limited time only, both urging the individual to act fast.

Patent infringing pharmaceuticals

This is the unauthorised manufacturing of patented[32] pharmaceuticals. Often the consumer does not receive what they have ordered, or the product could be damaging to the individual's health in the form of counterfeit medication[33]. This has a negative effect on the pharmaceutical industry, as well as indirectly affecting other industries as a result.

31 DoS: interrupts access of users to a system by submitting so many superfluous requests such that day-to-day activities cannot be accomplished.

32 Authority or license from the government granting the right, for a set period of time, to exclude others from the making, using or selling of an invention.

33 Deliberately mislabelled medication, medication with the wrong ingredients, fake packaging or the wrong quantity of ingredients in a medicine.

Crimes in the transitional cybercrime sector include:

Cryptojacking

(also known as malicious cryptomining): is a new threat since the emergence of cryptocurrencies. Criminals hide software on a computer or mobile device and uses the machines central processing unit (CPU) power to mine forms of online money, without the user's consent or knowledge. Instead of building a dedicated cryptomining computer, hackers use cryptojacking to steal computing resources from their victim's devices. With all these resources added up, hackers are able to compete against sophisticated cryptomining operations without the costly overhead. Symantec 2019 estimate over 69 million cryptojacking events have occurred between 2017 and 2018. In 2018, enterprises were also targeted with the WannaMine cryptojacking script, which uses Eternal Blue exploit made famous by WannaCry to spread through enterprise networks, rendering some devices unusable to high CPU usage[34].

Telephony fraud

Through the use of telecommunications products or services, the goal is generally to scam people out of money or retrieve private and confidential information from individuals. Examples include subscription fraud, overbilling, tariff plan abuse, international revenue share fraud and voice spam and scams.

ATM skimming

This is placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine. Criminals do it by planting a device on a ATM. The criminals have become very astute at creating them, often from plastic or plaster, so that they blend in to the ATM's façade. The device used is often a realistic-looking card reader placed over the factory-installed card reader. Customers insert their ATM card into the phony reader, and their account information is swiped and stored on a small attached laptop or cell phone or sent wirelessly to the criminals waiting nearby[35].

Card fraud

This is an umbrella term, with many sub-categories. In a broad sense however it is the unauthorised purchase of goods and services using stolen credit or debit card details. There are several different types of card fraud but they all share the same goal of financial gain. An indirect cost that must get a mention when dealing with card fraud is the cost of fraud management. There is also an additional cost as a result to businesses and to society in the form of increased management services.

Formjacking

Is a detection for the use of malicious JavaScript code used to steal credit card details and other information from payments forms on the checkout web pages of e-commerce sites. Whilst formjacking is not a new technique it has seen a dramatic increase since mid-August 2018. Formjacking works when a customer on an e-commerce website clicks "submit" or its equivalent after entering details into a website's payment form. Malicious JavaScript code is then used to steal payment card details and other information such as users name and address. This information is then sent to the attacker's servers. The attacker is then able to use the information to commit payment card fraud or to sell the information on the dark web. Third party services used by online retailers such as chatbots or customer review widgets were the main target in 2018[36].

Remote purchase fraud

When making a transaction, the card being used does not physically have to be present, for example, when shopping online (e-commerce) or placing a mail order over the phone. Typically, only the cards details are required. These details can be obtained electronically through phishing or the theft of one's details through a business that they have associated with.

34 Symantec 2019 Internet Security Threat Report
35 Taking a trip to the ATM?
36 Similar to phishing and vishing except a mobile device is used. The victim receives a SMS message which has a link attached however if clicked into, a Trojan horse (destructive programme) is downloaded onto the mobile device.

Traditional crimes that are now utilising cyber:

Social welfare fraud

Claiming benefits that an individual is not entitled to. Examples include, working full time while claiming Jobseekers Benefit or Allowance.

Tax fraud

The intentional act of evading tax. This is not to be confused with tax avoidance, which is minimising one's tax liability within the law.

Grant Thornton International Limited (GTIL)

We are Grant Thornton

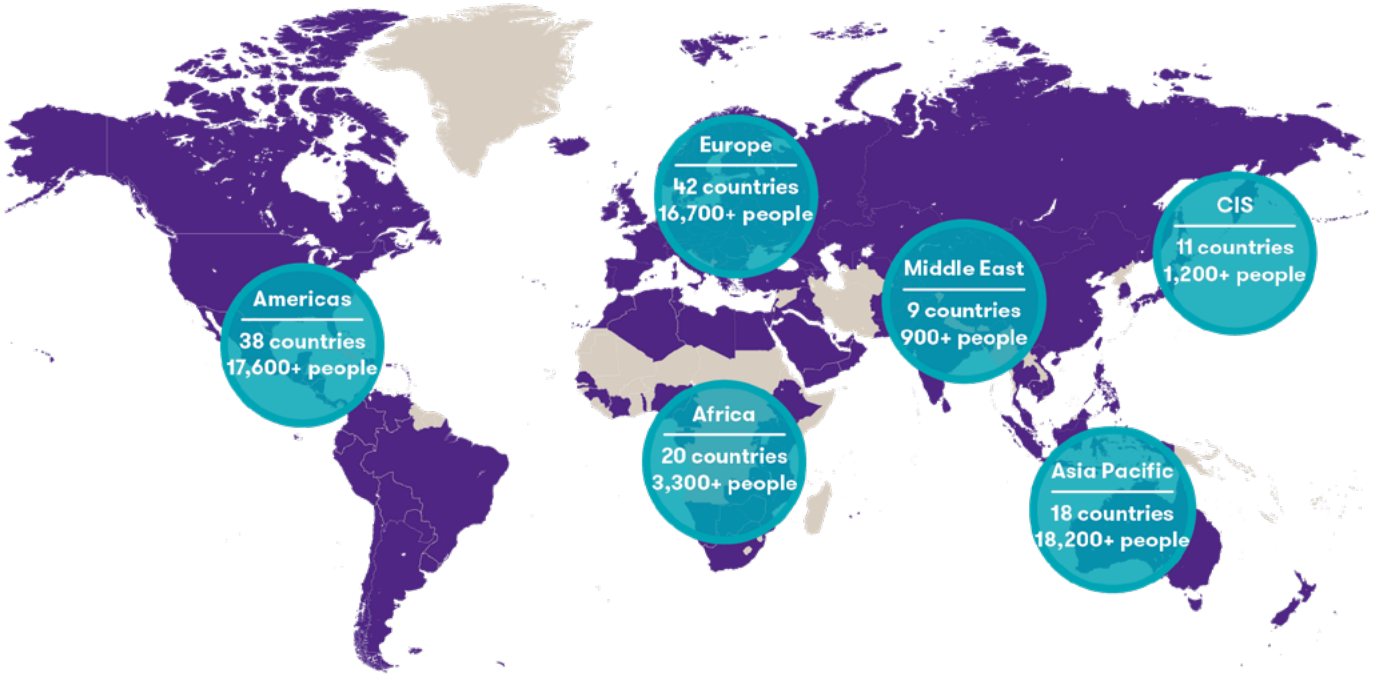
Grant Thornton is Ireland's fastest growing professional services firm. With over 1,500 people in 7 offices across Ireland and 58,000+ located in nearly 140 countries around the world, we bring you the local knowledge, national expertise and global presence to help you and your business succeed – wherever you're located. We deliver solutions to all business challenges. Clients choose us because the breadth of financial and business services they need is available, delivered innovatively and always to the highest standards. At Grant Thornton we are committed to long term relationships.

Grant Thornton operate from offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

About Grant Thornton International Ltd (GTIL)

We're a network of independent assurance, tax and advisory firms, made up of 58,000+ people in nearly 140 countries. For more than 100 years, we have helped dynamic organisations realise their strategic ambitions. Whether you're looking to finance growth, manage risk and regulation, optimise your operations or realise stakeholder value, we can help you.

We've got scale, combined with local market understanding. That means we're everywhere you are, as well as where you want to be.



Our distinctive client experience sets us apart

USD5.76bn (2020 revenue) | 58,000+ people | 750+ offices | 138 countries

Further information

Further information

To find out how Grant Thornton may be of assistance to you and your business, contact us.

Mike Harris
Partner,
Head of Cyber Security
T +353 (0)1 436 6503
E mike.harris@ie.gt.com

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

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

Martin Elliott
Associate Director,
Forensics & Cyber
T +353 (0)87 357 8751
E martin.elliott@ie.gt.com

Dublin
13-18 City Quay
Dublin 2
D02 ED70
T + 353 (0)1 680 5805

Belfast
12-15 Donegall Square West
Belfast
BT1 6JH
Northern Ireland
T +44 (0)28 9587 1050

Cork
14 South Mall
Cork
T12 CT91
T + 353 (0)21 494 9450

Galway
Ground Floor
Merchant's Square
Merchants's Road
Galway
H91 ETN2
T + 353 (0)91 533 924

Newbridge
Suite 3 and 4
Courtyard House
Newbridge
Co. Kildare
W12 DT89
T + 353 (0)45 449 322

Limerick
Mill House
Henry Street
Limerick
V94 K6HH
T +353 (0)61 312 744

Longford
2 Church Street
Longford
Co Longford
N39 W1X7
T +353(0)43 334 1900