Groups Report

Cyber Crime in Ireland

Group B:

Jack O’Connor	15394446	Introduction and Solutions
Joseph Davies	15530133	Cyber Crime: Why is it Growing?
Seán Jackson	15548377	Cyber Crime: Impact on Ireland
Michal Durinik	15737195	Cyber Crime: Irish Approach
Kieran Flynn	16334663	Cyber Crime: EU Approach

15th February, 2019

No plagiarism statement

I/We declare that this material, which I/We now submit for assessment, is entirely my/our own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my/our work. I/We understand that plagiarism, collusion, and copying are grave and serious offences in the university and accept the penalties that would be imposed should I engage in plagiarism, collusion or copying. I/We have read and understood the Assignment Regulations. I/We have identified and included the source of all facts, ideas, opinions, and viewpoints of others in the assignment references. Direct quotations from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the source cited are identified in the assignment references. This assignment, or any part of it, has not been previously submitted by me/us or any other person for assessment on this or any other course of study.

I/We have read and understood the referencing guidelines found at http://www.dcu.ie/info/regulations/plagiarism.shtml , https://www4.dcu.ie/students/az/plagiarism and/or recommended in the assignment guidelines.

Abstract

In the following report we will outline the serious impact that cyber crime has had in Ireland in recent years. The overall purpose of this report is to find the main reasons why cyber crime is so rampant in Ireland and what can be done to prevent it in the future. During our research we found some clear indications as to why cyber crime is widespread amongst Irish companies. Irish people and businesses are lacking in knowledge of the dangers of cyber crime. We look at the alarming figures that show how vulnerable Ireland is and why this may be happening. We look into the impact that these cyber crime attacks have had on Ireland and Irish companies. In addition, we will be looking at the Irish and EU approaches to tackling cyber crime. Possible solutions to cyber crime in Ireland are also explored on different levels. Companies vary in size and we look at the possible implementations these companies can make in order to reduce cyber crime and the impact it may have on these businesses. We aim to give multiple steps that Irish businesses can take to improve their cyber security. There are many suggestions throughout our report that can be implemented by any company in order to improve their cyber security.

Introduction and Background

Cyber crime is the act of carrying out criminal activities through the means of a computer or the internet. These crimes include phishing, hacking and spamming. The people who carry out these crimes are commonly referred to as ‘hackers’. The end goal for a hacker is usually to obtain some private or personal information that will in turn make them money. This could include getting bank details to steal money or stealing private information from businesses.

In the last two years in Ireland 61% of businesses have reported suffering from cyber crime. This is almost double the global figures for the sametime frame, which is 31%. These figures show that Ireland is being targeted more by hackers and they are succeeding at an alarming rate. The number of reported cyber crime attacks on Irish businesses has increased from 44%, which is an increase of 17%. The rate at which these crimes are rising is worrying for all Irish businesses. As a result of all these crimes, there are many businesses losing large amounts of money. Approximately 1 in 10 Irish businesses have lost upwards of €4 million due to cyber crime. Figures also show that 66% have lost up to €810,000.

Ireland is a clear target for hackers and there are many vulnerabilities amongst Irish businesses. These figures raise many questions about the prevention of cyber crime in Ireland. Do these businesses know how to prevent such attacks ? Do they even care about cyber security ? Irish businesses and Irish people need to come up with solutions to protect their companies and customers and remove these vulnerabilities.

Cyber Crime: Why is it Growing?

Cyber Crime is an industry that is becoming increasingly popular year after year, so much so that its worth worldwide is greater than that of the drug industry. When compared to other EU countries Ireland is more vulnerable to Cyber Crime which is down to a number of reasons, in particular a lack of foresight on behalf of Irish Companies. Despite numerous warnings from cyber security experts, they have repeatedly failed to implement appropriate security measures or even properly update software. Employers at these Companies aren't educated enough on cyber security or how to prepare against a cyber attack and do not seem interested in training their employees about it's dangers or investing in appropriate protection.

It has got so bad that a report towards the end of 2018 discovered that more than a third of Irish Companies did not even have a Cyber Security Policy in place. The report found that a further fifth of these Companies admitted that their security needed improvement or that they were completely insecure and unprepared for a Cyber Attack. The average time taken for Irish Companies to identify a Cyber Breach was found to be 191 days, with some not even becoming aware they had been breached until their data was sold on the Dark Web. The breaches are thought to be a result of the use of 'fileless malware' (malicious software that runs in memory and is much harder to detect), which leads to exploits such as ransomware.

A further reason for its increased growth is because the amount of cyber-dependent crime that is reported to An Garda Síochána, is relatively low in comparison to that which is dealt with by private cybersecurity companies. It is estimated that less than 5% of Cyber Crime is actually reported to the Gardai. With so little of it reported it leaves them unable to inform the wider community of these problems. One of the main reasons for these crimes going unreported is that Irish Companies are under the assumption the Gardaí wouldn't be able to do much to help. They also fear being embarrassed and that it would damage their brand. They do not wish for it to be a known fact that they weren't able to deal with a Cyber Breach or that they weren't prepared for one in the first place, especially when it comes to companies who store their customers private information.

Cyber Crime: Impact on Ireland

The impact of cyber crime in Ireland has led to large attacks on Ireland's public services such as the HSE, which is Ireland's health service and the revenue commissioners, which is responsible for Irish tax. There were over 5000 cyber attack events (Health Service Executive, 2017) in one hospital alone. These hackers would use ransomware to freeze patient files and blackmail them into paying for the files. This forced the Irish government to reboot their internal network (Health Service Executive, 2017) costing them time and money.

The impact of cyber attacks on businesses is enormous, as more than 10% of Irish businesses hit by cyber attacks in the past two years have lost upwards of four million each (Irish Independent, 2018). This fraud is exacerbated by the final cost of the cyber crime and dealing with the consequences (Irish Independent, 2018). Furthermore, two thirds of Irish businesses affected said they had spent as much as the original crime cost, or more, dealing with the cyber attack and conducting investigations (Irish Independent, 2018) to track down the source of the crime. These investigations would be long winded with many companies clueless who conducted the cyber attack.

The unsettling side to cyber crime in Ireland, is the fact that many companies do not even know if they have been attacked. 18% of companies surveyed in the Magnet Networks Cyber Security survey stated that, they were “Unsure” if they had fallen victim to a cyber security breach (Irish Independent, 2018). Mark Kellett CEO of Magnet Networks states. “This is worrying”. "As in the world of cyber-attacks, you are either totally secure or vulnerable in some way.” (Irish Independent, 2018).

Cyber crime has now overtaken asset misappropriation as the leading economic crime in Ireland (Irish Independent, 2018). Cyber crime in Ireland now accounts for 29% of all economic crimes perpetrated against firms (Irish Independent, 2018). Irish companies need to start taking cyber crime more seriously, as a massive 48% of businesses have no cyber security policy in place whatsoever (Irish Independent, 2018). This is crazy considering Ireland is one of the top business and technology hubs in Europe.

Cyber crime in Ireland not only affects businesses and firms, but Irish homes and citizens are just as vulnerable if not more to cyber attacks. Many people are unaware of what cyber security even means or how to look for signs of a cyber attack. Irish citizens need to be educated when it comes to keeping their data safe and secure. Implementing a system to raise awareness of the growing cyber crime network and how to defend yourself against these hackers is essential, especially for the less “tech savvy” folk out there.

Citizens are having their data stolen every day with a mere 5% of the cyber attacks being reported to the Gardaí (The Irish Times 2018). Ireland should aim to have the majority of the nation up to speed on cyber crime within the next 5 years, in order to have any chance of slowing down the already enormous cyber crime network.

Cyber Crime: Irish Approach

Cyber attacks from February of the last year against HSE, SafeFood, the Oireachtas and some other local authorities in Ireland lead to increased talks about the security (The Irish Times, 2019). Apart from the initial damage, it exposed vulnerabilities in the system to further attacks, which raised more awareness about the issue.

As Taoiseach Leo Varadkar said, he believed that Ireland got spared of some of the big external attacks (The Irish Times, 2019). The "Wannacry" attack on National health service in Britain was very devastating and luckily avoided here.

It could be one of the reasons for the slow development of cybersecurity in Ireland in the past years, but it is fast improving.

The National cyber security centre was formed only in 2015, and it is still a relatively new organisation. Its primary focus is to protect critical national infrastructure as well as businesses and citizens.

Industrial Development Authority, which is responsible for attraction and retention of investment into the country funded new security cluster called Cyber Ireland. It will be located and run from Cork Institute of Technology and will represent companies such as (Dell EMC, McAfee, IBM) working in the cybersecurity field, and it's 6000 employees. It is the first time in Ireland, that government-financed such initiative directly (The Irish Times, 2018).

In and around Cork city are located nearly 60 Irish-owned cybersecurity companies and 40 multinational companies (The Irish Times, 2018). It is a good indicator of the growth in the sector. One of the challenges with such rapid growth is sourcing talented engineers as unemployment in this field is close to zero percent (The Irish Times, 2018).

There are definite improvements in 2019 and plans going forward. However, not only in Ireland, the development of new law often lags behind social and technological changes, which is especially true in the cybersecurity sector (Old Laws, New Crimes, 2016).

It will take some time to develop proper legislation.

Cyber Crime: EU Approach

While other countries are considering their membership to the European Union, Ireland will be a pivotal ally of Europe as the only native English speaking country. However, this also means that they are equally as vulnerable to cyber attacks as their fellow European counterparts. Citizens of Europe were victims of cyber attacks on their digital transactions 30% more often at the beginning of 2018 than upon the previous year(Computer Weekly 2018). Consequences of these kind of actions include having personal data such as bank details leaked & unauthorised monetary transactions.

Not only are members of the public vulnerable, but equally so are the public officials & services of these European powers. Most significantly of all members, Great Britain, Germany and France are among the highest attacked countries not only in Europe, but also the entire world(CSIS 2018). These incidents include attacks taken against members of the german parliament, investigators into incidents such as the Novichok poisonings in Salisbury and supply chains for British industrial firms. Although incidents involving the United Kingdom will cease to be a concern once they leave the European Union(BBC 2018), it's still important to highlight how Irelands fellow powers have been impacted by cyber crime.

In saying that, the European Union is actually more of an asset to the Irish government in combating cyber crime than a hindrance. The EU has taken a number of significant steps in the past few years to stunt the growth of cyber attacks across the continent. In 2013 they launched a directive with the aim of stifling major cyber attacks on information systems by encouraging their member states to introduce new laws and further punishments for those responsible for these kinds of attacks(European Commission 2019). The European Commision in 2017 outlined the impact of this directive by outlining the numerous punishments that can now be applied to offenders of crimes such as illegal data interception and system interference(Report to European Parliament 2017). Thus showing significant progress in their goal of stomping out criminal activity online.

Although, this directive isn’t the only technique the EU have used to combat cyber crime across the continent. In 2013 the European Cybercrime Centre was also established. The primary goal of this centre is to design and implement strategies and operations aimed at combating cyber crime(European Commission 2018). This involves cooperation alongside fellow member states and the ENISA to ensure investigations into cyber criminal activities are performed effectively and healthy networking practices are maintained across the continent(Taylor Francis 2014). With a number of methods being created and implemented across numerous countries in Europe, the EC3 has to stay alert to what trends are arising among hackers and identify counter measures that can be brought against them. And it would appear so far that they can achieve this successfully as the centre have been key figures involved in cases where hackers have been raided and subsequently arrested on cyber crime charges(BBC 2019).

Much like the EC3, the European Network and Information Security Agency(ENISA) is concerned with new trends within security activities. Although they are not primarily an anti cyber crime establishment, since they also look to encourage innovation in networking and security, they also look for ways to implement new policies that can achieve greater network security across Europe(ENISA 2013). They also look to work with member states to improve their capacity to investigate security issues and follow through on actions following breaches. Alongside the EC3 and the information systems directive, each of them serve as a significant approach to help countries such as Ireland in the combat against Cyber Crime.

Possible Solutions

Low-tech solution: A simple low tech solution would be to make employees of companies aware of the dangers of cyber crime. By making people aware of how serious these offences are and the possible consequences, they will be more likely to take caution with any information that they have. Encouraging any employee to simply change their passwords regularly would be something that could be simple enough to prevent a leak of information. These solutions are low cost and would be relatively simple to implement.

Mid-range solution: It would be possible to reduce the amount of attacks by having an updated security system. There are constantly new ways for hackers to obtain information. A hacker just needs to find one weakness in a security system. If a business is constantly updating their security system it will make a more difficult defence system for a hacker to penetrate. Having a strong and secure system is pivotal to retaining all sensitive or private information that a business may have. This implementation may be costly to execute but it will provide to be beneficial if it does the job correctly. Keeping unwanted hackers away from all information is the main aim and having a strong security system should be a main priority for all businesses.

Long-term solution: For many businesses that may already be subject to cyber crime it may be beneficial to completely restructure their business. Many companies have multiple vulnerabilities in their systems and the means by which they store their data. A complete overhaul may be too much for smaller companies to fulfill as they simply couldn't afford the complete overhaul and restructure. For other larger companies it could be a move that sees them protect their data and assets and in turn makes them more money. Being able to log all transactions and logins from every company account and computer would be incredibly beneficial for a business. An unauthorised login or transaction may become more visible and will become more likely to be prevented.

Discussion

For many companies, large or small, there is many difficulties when it comes to improving their security to reduce cyber crime. One of the main things for a company to consider is the cost. Will it be more beneficial to spend the money to strengthen the security or is it just not plausible to spend money that is simply not there ?

There are plenty of advantages for implementing any of the suggested solutions. As there are more than one third of Irish businesses with no cyber security it would be beneficial for any of these businesses to create one. There seems to be a lack of knowledge towards the seriousness of cyber crime and the people of Ireland are failing to acknowledge that it even exists. Having any sort of cyber security in place could prevent an attack and in turn protect a company from losing money and potentially losing customers. Having a good reputation for protecting information could be largely beneficial to any business and could increase profits and potentially allow for further expansion. The main goal would be to decrease the enormous rates at which Irish businesses are suffering cyber crime attacks.

With all discussions there are two sides. Looking at the disadvantages to these possible solutions there is one major factor, which is cost. Many Irish businesses simply cannot afford to upscale and upgrade their security to a high enough level. The cost of restructuring and maintaining a high level of security could be out of the picture for some smaller businesses. This in turn leaves some people or businesses more vulnerable as they don’t have much options in terms of other ways to prevent cyber crime. Another factor to consider is that a company may spend a lot of money on an area they think is vulnerable when it may in fact be protected. Many companies may feel like they are spending too much money without getting anything in return or seeing the benefits of upgrading their security.

Recommendation

It would be recommended to implement a scheme made by a company or the Department of Justice and Equality which would educate businesses on how to improve cyber security and reduce cyber crime. By showing the effects of cyber crime and the possible outcomes people will take it more seriously. It is incredibly important for businesses to be protective of their data and by knowing the risks with having no security they can be better protected. This scheme could be basic for companies starting out or complex for companies wishing to improve or restructure their security networks. This option would be beneficial as it wouldn’t place all of the costs on the businesses themselves. The government has a right to protect the people of this country and this also includes the businesses that operate in this country.

Conclusion

In conclusion, cyber crime inside of Ireland is growing, as it is throughout the rest of Europe and most of the modern world. It is having an impact of many different backgrounds, in many different sectors and numerous areas of the country. As a result, the impact of cyber crime is an extreme concern for both the public, politicians and public figures alike. In saying that, there is being steps taken to stunt the growth of cyber crime. Initiatives being taken by companies, the government and the European Union together to secure themselves from cyber attacks and enforce laws and punishments upon those that are responsible. Although the rate of cyber crime may increase as the world and the country progresses further into the digital millennium, there are important decisions being taken to ensure that Ireland is protected and that committers of these offences are stomp upon with righteous anger by law enforcement and the criminal justice system.

References

Health Service Executive (2017) *Over 5000 cyber attack events.* Available at: https://www.hse.ie/eng/services/news/media/pressrel/over-5-000-cyber-attack-attempts-discovered-in-one-hospital.html (Accessed: 12 February 2019).

Health Service Executive (2017) *Reboot their internal network.* Available at: https://www.hse.ie/eng/services/news/media/pressrel/over-5-000-cyber-attack-attempts-discovered-in-one-hospital.html (Accessed: 12 February 2019).

Irish Independent (2018) *More than 10% of Irish businesses hit by cyber attacks in the past two years have lost upwards of four million each.* Available at: https://www.independent.ie/business/irish/irish-companies-count-cost-of-rise-in-cyber-crimes-37020440.html (Accessed: 7 February 2019).

Irish Independent (2018) *This fraud is exacerbated by the final cost of the cyber crime and dealing with the consequences.* Available at: https://www.independent.ie/business/irish/irish-companies-count-cost-of-rise-in-cyber-crimes-37020440.html (Accessed: 7 February 2019).

Irish Independent (2018) *Irish businesses affected said they had spent as much as the original crime cost, or more, dealing with the cyber attack and conducting investigations.* Available at: https://www.independent.ie/business/irish/irish-companies-count-cost-of-rise-in-cyber-crimes-37020440.html (Accessed: 7 February 2019).

Irish Independent (2018) *18pc "unsure" if they have been affected.* Available at: https://www.independent.ie/sponsored/the-economic-impact-of-cyber-crime-on-your-business-37161161.html (Accessed: 10 February 2019).

Irish Independent (2018). *"This is worrying," points out Magnet Networks CEO Mark Kellett. "As in the absolute world of cyber-attacks, you are either totally secure or you are vulnerable in some way."* Available at: https://www.independent.ie/sponsored/the-economic-impact-of-cyber-crime-on-your-business-37161161.html (Accessed: 10 February 2019).

Irish Independent (2018). *A massive 48pc of all businesses in Ireland still have no cyber security policy in place*. Available at: https://www.independent.ie/sponsored/the-economic-impact-of-cyber-crime-on-your-business-37161161.html (Accessed: 13 February 2019).

Irish Independent (2018). *Cyber crime was the top economic crime here, having overtaken asset misappropriation for the first time*. Available at: https://www.independent.ie/business/irish/irish-companies-count-cost-of-rise-in-cyber-crimes-37020440.html (Accessed: 13 February 2019).

Irish Independent (2018). *The latter now accounts for 29pc of all economic crime perpetrated against firms*. Available at: https://www.independent.ie/business/irish/irish-companies-count-cost-of-rise-in-cyber-crimes-37020440.html (Accessed: 13 February 2019).

The Irish Times (2018). *Less than 5 per cent of of cyber crime is reported to gardaí*. Available at: https://www.irishtimes.com/news/crime-and-law/less-than-5-of-cyber-crime-reported-to-garda%C3%AD-1.3353433 (Accessed: 14 February 2019)

(European Commission 2019) https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en (Accessed 7 February 2019)

(CSIS 2018) https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (Accessed 7 February 2019)

(Computer Weekly 2018) https://www.computerweekly.com/news/252441231/European-cyber-attacks-up-nearly-a-third-in-first-quarter-2018 (Accessed 7 February 2019)

(Taylor Fowler 2014) https://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261 (Accessed 14 February 2019)

(BBC Brexit 2018) https://www.bbc.com/news/uk-politics-39143978 (Accessed 14 February 2019)

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Accessed 10 February 2019)

(European Commission 2018) https://ec.europa.eu/digital-single-market/en/blogposts/europols-european-cybercrime-centre-quick-insight-combating-cybercrime (Accessed 10 February 2019)

(BBC Raids 2019) https://www.bbc.com/news/uk-england-47072313 (Accessed 13 February 2019)

(ENISA 2013) https://www.enisa.europa.eu/about-enisa/mission-and-objectives (Accessed 14 February 2019)

(Pwc.ie. 2018) https://www.pwc.ie/publications/2018/economic-crime-survey-2018.pdf

[Accessed 10 Feb. 2019].

https://www.independent.ie/business/dublin-information-sec/fear-of-brand-damage-stops-firms-reporting-cyber-crime-37251758.html

https://www.techcentral.ie/a-third-of-irish-businesses-lack-a-cyber-security-policy/

https://www.independent.ie/irish-news/news/gangs-know-ireland-is-vulnerable-and-cyber-crime-is-more-valuable-than-drugs-experts-warn-36372290.html

https://www.siliconrepublic.com/enterprise/cybercrime-ireland-pwc

https://www.independent.ie/business/technology/news/cybercrime-rise-is-threat-to-ireland-inc-flanagan-37422540.html

(The Irish Times 2019) Cyber attacks from February of the last year against HSE

https://www.irishtimes.com/news/politics/oireachtas/taoiseach-revenue-commissioners-and-hse-at-cyber-attack-risk-1.3391285 (Accessed 14 February 2019)

(The Irish Times, 2018)

https://www.irishtimes.com/business/technology/ida-to-fund-new-cybersecurity-cluster-to-put-ireland-on-global-map-1.3728777 (Accessed 14 February 2019)

(Old Laws, New Crimes, 2016)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2729204 (Accessed 14 February 2019)