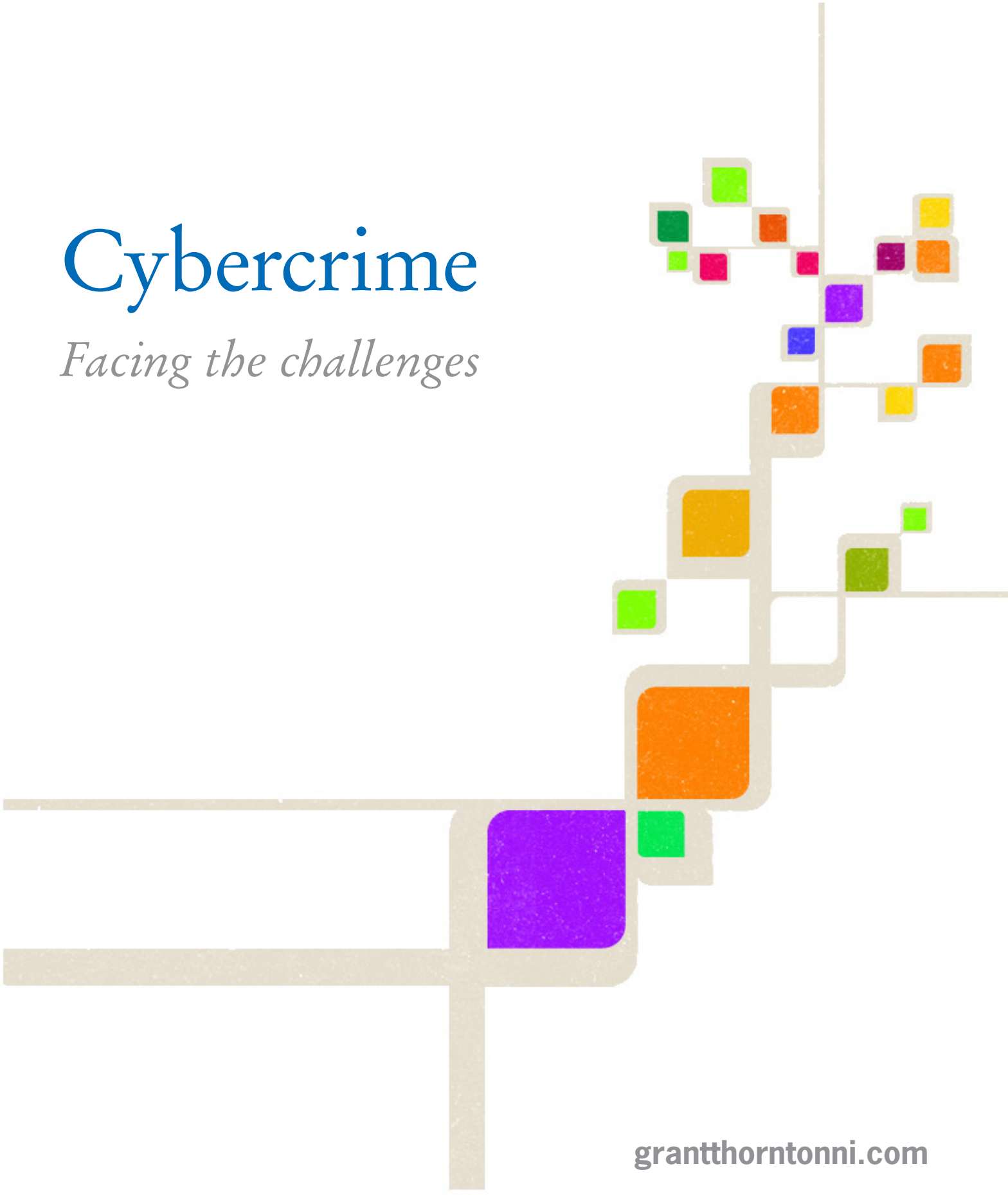
Grant Thornton

An instinct for growth™

Cybercrime

Facing the challenges



grantthorntonni.com

Contents

Executive summary

"The lesson from both of these attacks is clear: individuals, businesses and Government must be constantly vigilant and ensure that our systems evolve to meet the ever-growing threat."[1]

Tánaiste and Minister for Foreign Affairs & Trade, Mr. Eamon Gilmore T.D.

Data is increasingly playing an important part in the global economic landscape. As we seek to provide more efficient services or gain more meaningful insights into consumer behaviour, we are collecting and storing more and more information. This information has become a valuable commodity to many and as such the collection and use of this data is a growing area for the international community in terms of legislation and enforcement.

As this new economy continues to grow, so too does the associated shadow economy. Throughout this report we have identified the increasingly global nature of illicit trade, but it is especially relevant in the area of cybercrime. Recent high profile examples of personal data theft in Ireland and internationally has pushed the issue of data theft and cybercrime to the forefront of global debate.

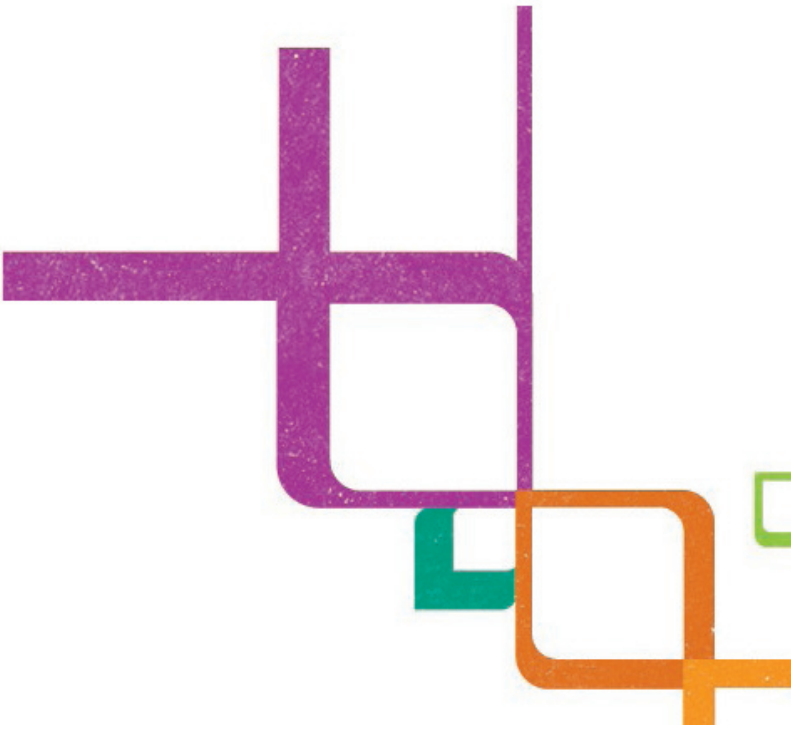
Many governments have in fact identified cyber security as one of the top threats to their country alongside natural disasters, international terrorism and military invasion.

The development of ICT has broken down borders and technology continues to develop rapidly. However, the legislative and enforcement frameworks continue to lag behind making it difficult to prevent and track data breaches.

The rise of cybercrime is not disputed. However, the wide varieties of estimates, which range from a few billion euros to hundreds of billions, reflect the inherent difficulties in measuring the true economic impact.

For Ireland with its focus on foreign direct investment, in particular in the areas of financial services and information technology, this will be a key battle ground against the growth of illicit trade to ensure that firms feel confident in the regulatory environment and government response that protects its strong reputation.

In order to plan the appropriate level of resources for both governments and firms to fight cybercrime, we need to create a broader understanding of the importance of data and examine the key characteristics and drivers of the global and Irish markets for illegal data.



[1] Pamela Newenham, 2013, "Tánaiste says data breach a wake-up call on cybercrime", The Irish Times 16 November. Available from www.irishtimes.com

Types and characteristics of cybercrime

Definition of cybercrime

In assessing the current state of cybercrime, we need to consider what exactly constitutes a cybercrime.
The standard definition calls it "criminal activities carried out by means of computers or the internet".
However, it is difficult to distinguish between computer-based and computer-aided crimes. In this technologically driven age virtually any crime may have be aided or facilitated by technology, whether using a website to hire a hitman[2] or using the internet to research a crime . We will not attempt to give a complete description of all cybercrimes, instead we focus on pervasive, large scale and automated types of data breaches where data (personal or otherwise) has been the subject to unauthorised access, collection, use or disclosure for monetary gain.

The cybercrime of interest can be categorised into a number of areas of focus:

- **identity theft** – cyber criminals obtain personal data from individuals (i.e. address, date of birth or bank account details) and exploit this online by opening fraudulent accounts (for example, bank accounts and mortgage applications). In many cases, the victims are not even aware of a problem until the impact becomes severe;
  - online/internet scams: cyber criminals obtain financial or other valuable information by fraudulent means, usually by tricking individuals through interrelated online scams which include;
  - online purchase fraud: such as making people pay for goods they do not intend to despatch;
  - pharming: redirecting website traffic from a legitimate website to a fraudulent website. This can also be used to infect an individual's computer with malware and compromise online accounts (for example, online banking);
  - phishing: this is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy party in an electronic communication. For example, sending fake money-transfer requests from foreign countries to thousands of e-mail accounts;
  - spear phishing: highly-personalised fake e-mails targeted at a single individual. This is often used to target high net worth individuals or as the first step in a wider attack to compromise data in an organisation;
  - vishing (voice phishing): is similar to phishing type of scam using voice messages that paper to be from a trustworthy party to defraud customers; and
  - cyber theft from business: cybercriminals steal data or revenue directly from businesses. This usually involves unauthorised access and targeting of company online systems, websites, databases, accounts and monetary reserves. Recently, the reputational impact of a successful cyber theft has become critically important for Irish businesses[4].
- **cyber extortion**: this involves an attack or threat of attack against a business, coupled with a demand for money to avert or stop the attack. This includes holding a company to ransom often through deliberate denial of service. For example, by using malware to overwhelm a company's website with internet traffic or by manipulating website links, which could lead to substantial brand damage (for example, by redirecting links for a retailer website to a pornography website). In recent years, cyber criminals have targeted many Irish organisations

[2] Gavan Reilly, 2012, "US woman gets six-year sentence for hiring 'Lying Eyes' hitman", The journal.ie 16 January. Available from www.thejournal.ie
[3] RTE News, 2005, "Whelan given life sentence for wife's murder", RTE News 12 April. Available from www.rte.ie
[4] Conor Pope, Elaine Edwards, 2013 "Over 1.5 million affected by Ennis data breach", The Irish Times 12 November. Available from: www.irishtimes.com

using so call "ransomware" that is used to encrypt the victim organisation's data. The cybercriminal then demands money for the decryption key[5].

- **industrial espionage**: this takes many forms, such as a competitors gaining authorised access to confidential data to gain competitive advantage or individuals gaining insider knowledge for financial gain. This could include finding out a competitor's bid price or becoming aware at an early stage of a possible merger or acquisition.
- **online intellectual property theft**: cybercriminals, often sponsored by competitor organisations or, increasingly, countries' governments, steal designs, technical specifications, trade secrets, process information or detailed methodologies, which can quickly erode competitive advantages. The impact of this cybercrime can be particularly strong in a small export driven economy like Ireland.

These are the cybercrimes that are dramatically increasing in occurrence and are having the greatest economic impact both in Ireland and internationally. It is important to note that the financial impact of such cybercrime comes in two forms:

- **transfer of funds**: for example, through the transfer of money from online bank accounts or the use of compromised credit cards.
- **the intrinsic value of the data stolen**: for example personal financial data or credit card details can be traded on underground sites on the internet[6]. In fact, a valid stolen credit card can be worth as much as $100 online depending on the amount of information available with the card[7].

[5] An Garda Síochána, Garda Warning in relation to Computer Scam "Police" Trojan – Ransomware

[6] Rupert Steiner, Sam Greenhill, 2014, "Turmoil at Barclays as whistleblower reveals 27,000 customers personal details were sold on black market", 9 February, This is Money. Available at: www.thisismoney.co.uk

[7] Ken Westin, 2013, "Stolen Target Credit Cards and the Black Market: How the Digital Underground Works", 21 December, The State of Security. Available at: www.tripwire.com

Key drivers to cybercrime

By applying the traditional economic forces of supply and demand to the economic landscape of data we can begin to understand the true drivers behind the growing incidences of cybercrime.

Supply

On the supply side, it is the institutions (and some cases the customers of the institutions) in both the public and private sectors that are the producers of the commodity (i.e. data), whereas the cybercriminals act as agents who procure and sell these products at the going market price. It is these agents supply of this illicit product which creates the actual market itself. Below we have given a profile of breach agents collated by Verizon.

Clearly the vast majority of breaches of cyber security are committed by agents external to the organisation targeted. Historically, it has been felt that attacks committed by insiders had a greater financial impact on institutions. However, the sheer intensity of attacks recently coupled with the volume of data stolen would indicate, anecdotally at least, that the impact of attacks external to institutions is now much greater. This volume of data is no surprise: over the past decade organisations (and consumers) have dramatically increased the volume and quality of data that they produce. Whether it is a bank's information on its customers or an individual's data stored on a social networking site, the volume of valuable data that is potentially accessible through online channels has rocketed. Clearly the potential market is large and growing, as is increasing amount of information available online.

This has placed an increasing strain on the ability of organisations to protect both their and their customer's data from authorised access attempts. In fact, dramatically increasing spend on online security controls has not always protected organisations from falling victim to a data breach. Organisations who do not invest in online security will eventually fall victim to a breach, which will result in the company investing in security to protect their business anyway in addition to the direct costs of a data breach. It is therefore important that an appropriate balance is found.

There are a number of other factors that dramatically ease the acquisition and supply of illicit data that assist perpetrators of cybercrime. Primary amongst these is the fact that the risk of discovery remains low due to the ability to conceal their identity. This coupled with the lack of harmonised legislation across borders results in jurisdictional issues for law enforcement. In addition, the increasing sophistication of attackers, coupled with a commoditisation of exploitation techniques, has lowered the barrier to entry for cybercriminals. Fundamentally, for potential cybercriminals it is increasingly easy (and cheap) to instigate an attack, with the chances of being detected remaining low and even if they are detected the penalties are likely to be limited.

Demand

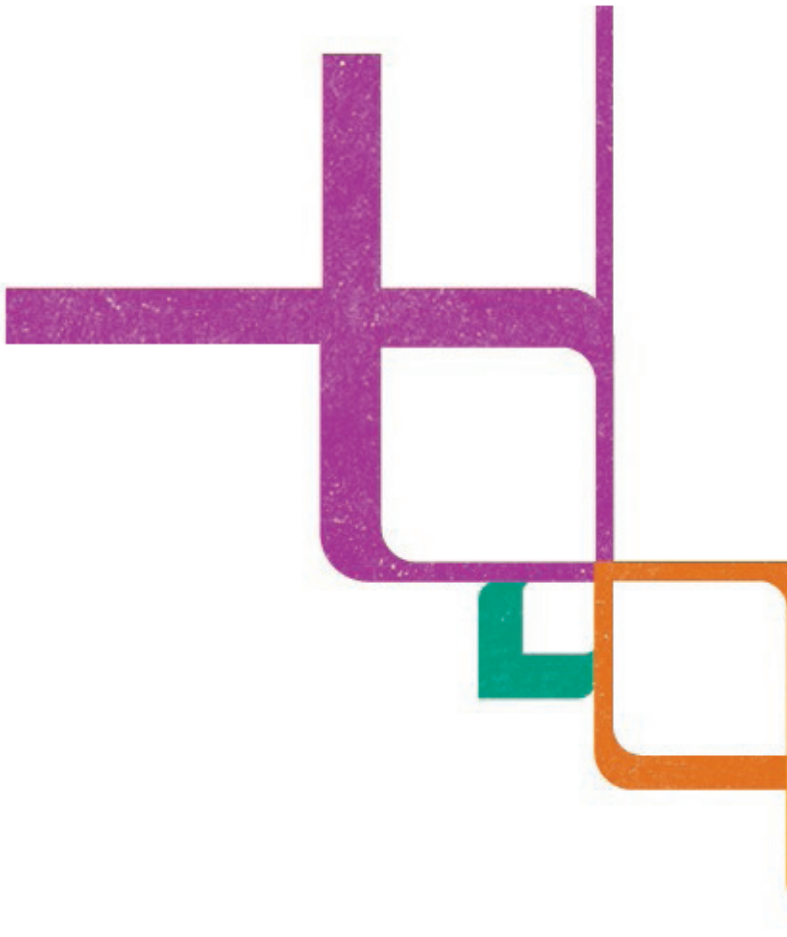
The continued increase in the size and scale of data breaches demonstrates the growing demand for this illicit information. The research indicates that for malicious cybercrime, unsurprisingly, it is financial motives that are the main driver in the commercial sphere.
However, for cybercrime in the public sector there are additional motivations such as access to intellectual property, military intelligence and insider information etc., which fuel the demand.

From our research we have seen the demand being

consumed by five key categories of consumers, each with different motivations and incentives. The table below gives a profile of each of these consumers.

Table 2.1 - Cybercrime consumers[8]

Consumer	% of total	Description
Organised crime	55%	With more than half of external breaches internationally being carried out by organised criminal gangs, this reflects the high prevalence of activities such as scamming, payment fraud, identity theft etc.
State affiliated	21%	State affiliated breaches are not necessarily motivated by financial incentives. They seek other types of information such as military, insider information, intellectual property or source codes.
Unknown	13%	Unidentified/untraceable breaches.
Unaffiliated	8%	Individuals not linked to other categories. Majority would be individual hackers or current employees.
Activist	2%	Activists form another important part of the threat actors within the cybercrime landscape. Such activists are more concerned with ideological motivations and as such are leaking this information to the public.
Former employee	1%	Former employee of organisation.



The international nature of the demand means that the potential impact on a small open economy like Ireland is not limited by the size of the Irish market demand.

[8] Verizon, Data Breach Investigations Report 2013

Trends in Irish crime

The area of cybercrime trends has and continues to change at an incredibly rapid pace. The increasing use and dependence on technology continues to be one of the major influences on both the domestic and international economic landscape. With each new year, new cybercrime trends emerge, further complicating an already challenging environment for businesses and legislators. This speed of change requires agility in their response that both business and government struggle to deliver.

Below we have outlined some of the key cybercrime trends affecting the global economy:

- "big data" technologies are increasing the effectiveness of attacks. The "big data" trend is driving organisations to gather increasing volumes of data from their operations and customers. The importance of speed to market means that many organisations with "big data" initiatives are not making the investments to ensure that this new data is secured appropriately. Increasing an organisation's ability to gain insight from its data very often leads to an increased risk of unauthorised access.
- organised criminals continue to be the main players. Over the past decade organised crime has been the main driver of cybercrime. This initially manifested itself in large automated attacks on the customers of financial institutions and online merchants. Recently, however, criminals have shifted their targets away from individuals to companies. They are focusing not only on stealing data from the institution's customers but stealing customer information directly from the institutions themselves. Because of this the frequency, size and cost of cyber-attacks are on the increase.
- financial motives continue to be at the heart of the increase in cybercrime. Cybercrime has been and continues to be a commercial endeavour driven by supply and demand. This is consistent with the fact that the most costly attacks for organisations tend to be those that are malicious or are criminal attacks. In addition, there is evidence to suggest that the US and UK companies who have a strong security position (posture, incident response and senior executive attention) have the greatest reduction in data breach costs.
- non-reporting of cybercrime by business and individuals continues to be an issue globally. Organisations are often concerned by the reputational impact of cybercrime. They do not want their customers to know that the security of their data has been compromised. This has resulted in a lack of information to accurately assess the financial costs of cybercrime and lead the increasing use of data breech disclosure legislation in many jurisdictions.
- mobile cybercrime. The dramatic increase in the proliferation of mobile devices like tablets and smart phones has opened new avenues of attack. The opportunities for cybercrime attacks on consumers using these devices are only beginning to be realised and it is likely that this is an area for future growth.

Irish trends

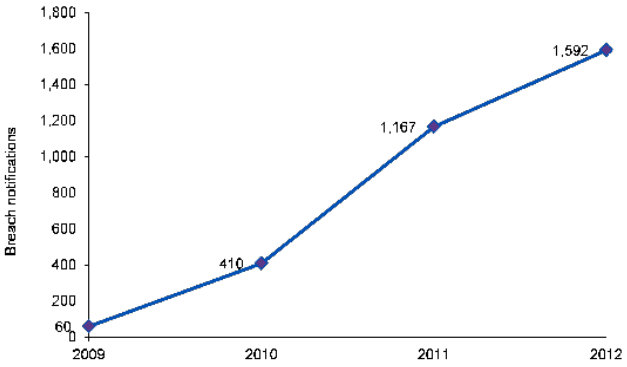
The increasing importance and commoditisation of information has resulted in the creation of an international market for such information. In terms of market trends, it is fair to say there is no sign that cybercrime is going away. There has in fact been a marked increase in the number of data breaches in terms of the frequency, size and cost both domestically and internationally.

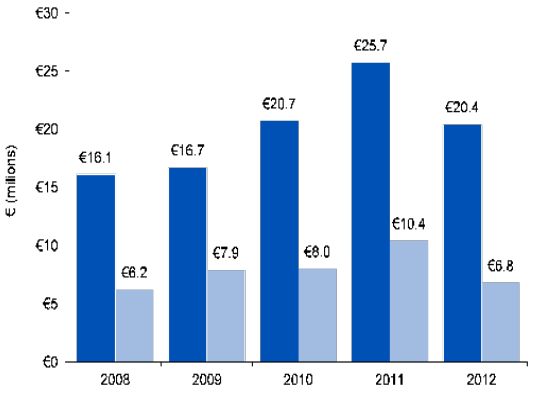
From an Irish perspective we have seen a continued rise in the number of security breaches. During 2012, the Office of Data Protection Commissioner dealt with 1,592 personal data security breach notifications[9], which is the fourth straight increase since the introduction of the Code of Practice in 2010. This is illustrated by Figure 2.1 over.

Figure 2.1 – Breach notifications (2009 – 2012)[10]

[9] Annual Report 2013, Data protection commissioner

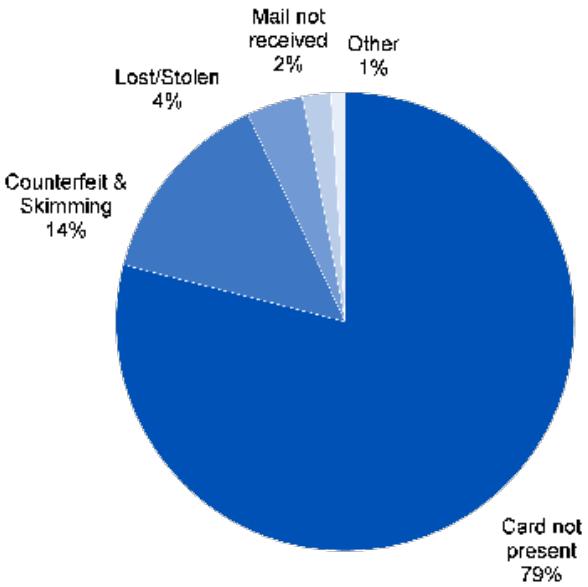
Figure 2.2 - Online payment card fraud in Ireland[12]





According to the annual report of the Data Protection Commissioner, although the "complexity of certain data security breaches increases it is the more mundane situation of correspondence being issued to an incorrect address that continues to account for the largest percentage of data security breaches".

It is important to note that although the majority of breaches reported are described as mundane related to operation failures. However, a general tendency of Irish organisations to not report data breaches if at all possible, coupled with a lack of sophistication and maturity in Irish organisation's security capabilities, would lead one to conclude that the level of data breaches in Ireland is substantially under reported.



Online payment card fraud

Online payment card fraud continues to be one of the most common and best understood types of cybercrime in Ireland. Data from the Irish Payment Service Organisation (IPSO) indicates that card fraud is estimated at €20.4 million, with 79% of this taking place with a card not being present at the time of payment (i.e. online)[11].

[10] Annual Report 2013, Data Protection Commissioner
[11] IPSO, 2013, "ROI Card Payment Fraud Statistics 2012"
[12] IPSO, 2013, "ROI Card Payment Fraud Statistics 2012"

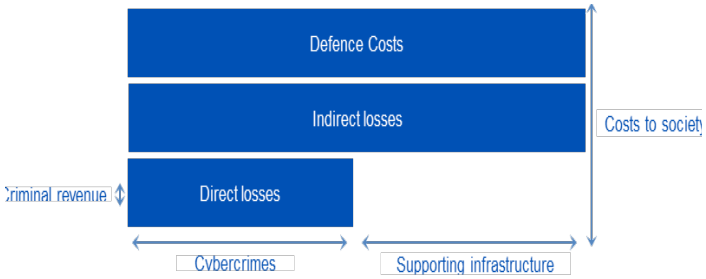
Costs of cybercrime

There are real costs to the economy of cybercrime. However, they can be difficult to quantify. The newness of the issue of cybercrime has resulted in widely varied estimates of the costs of international cybercrime ranging from €27 billion to €400 billion. Internationally, the average cost of a data breach to a company is €2 million per breach. For our nearest neighbour, the UK, the cost of data security breaches ranged from €200,000 to €6 million last year. In Ireland we have seen similar wide ranges.

Given such wide ranges in security breaches, we explored what makes up the costs of cybercrime both from a financial and non-financial perspective.

In considering these costs we have used a framework developed by an international team of scientists led by the University of Cambridge. This framework, together with data gathered by the Poneman Institute, has allowed us to identify the costs, associated losses and estimate what we believe to be a reasonable range of the cost of the issue for the Irish economy. We first identify the costs for individual businesses operating in Ireland[13] and then broader costs for the Irish economy as a whole.

Figure 2.3 - Costs of cybercrime[14]



Direct losses

The first element to this framework is direct losses. These losses relate to equivalent losses, damage or other suffering by the victim as a consequence of cybercrime. Primarily amongst these losses are notification costs and intellectual property costs, but they also include financial losses associated with money withdrawn from victim accounts etc.

Notification costs

For businesses there is a growing body of regulations that must be complied with regarding the collection and use of information about individuals. Many of these laws focus on the types of personal information that are subject to data breaches and the requirements of the organisation to notify individuals affected by a breach. Ireland itself has adopted a voluntary breach notification code ("Guidance and Personal Data Security Breach Code of Practice"). However, it is not legally binding.

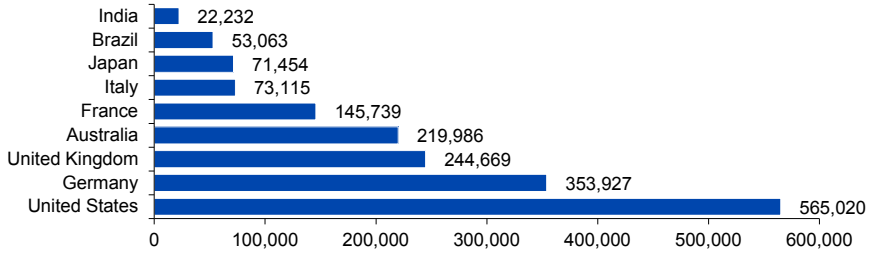
There are real costs associated with responding to a breach, which typically include IT activities, determination of the regulatory requirements, engagement of outside experts, and finally postal and follow up communication costs. Much of this is further complicated by the different requirements in different jurisdictions. The average cost to an institution can be as high as $565k in the USA and $244k in the UK[15]. If we take the average for the European countries reviewed, the cost to an Irish company would be in the region of €194k.

[13] We have worked from the fact that the Irish economy accounts for about 0.34 of the world GDP and scaled our national estimates up or down as appropriate

[14] Measuring the cost of cybercrime, University of Cambridge - 2012

[15] Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"

Figure 2.4 Notification costs per organisation '$



Intellectual property costs

It is likely that the greatest cost to a company is the loss of its intellectual property. Whilst this may not have a direct financial impact on its current profit and loss account, it can have a significant impact in the long term. The loss of intellectual property may not show up in a competing product for years. With companies investing heavily in research and development to build this intellectual property, a breach of its cyber security and the resulting loss of trade secrets could significantly impact on the company.

Defence costs

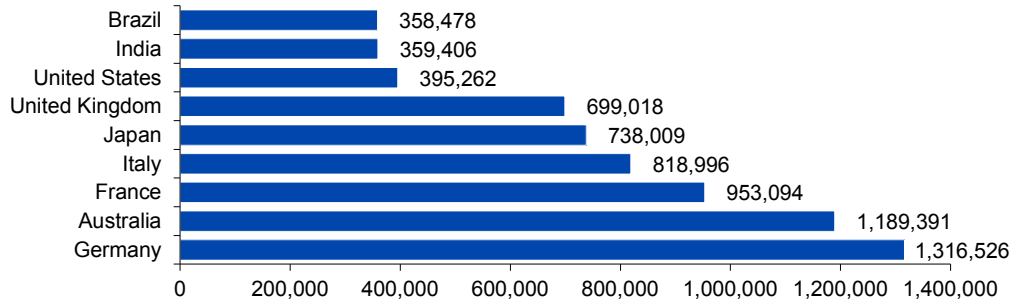
Defence costs are the monetary equivalent of prevention, detection and escalation costs which represent one of the most significant costs associated with cybercrime. As companies are increasingly concerned with ensuring the protection of its data they are spending more on data breach discovery and detection. Detection costs typically include forensic and investigative activities, assessment and audit services, crisis management and communications to executive management.

Germany has the highest defence costs per organisation at $1.3 million, with the Europe average also being significant ($946k)[16].

Loyaltybuild – Largest Irish data breach.
Loyaltybuild is an Ennis-based company that provides services to companies running holiday break promotions. It was hit by a major data security breach in late 2013. The breach involved the compromise of the personal details of about 1.5 million people across Europe. This included about 90,000 Irish customers of companies such as Axa, Clerys, ESB, Supervalu, and Pigsback. Initially, the company and clients including Supervalu and Axa had reassured customers that their personal data had not been compromised. But it was later acknowledged that this was not the case. Some of the personal information had been stored in unencrypted form and in some cases, credit card information was involved. Loyaltybuild ceased taking bookings on its websites and in its call centres in November when the Protection Commissioner began investigating the breach and the business did not recommence until March. During this time the company also had independent expert undertake an investigation into the cyber-attack. In addition, they invested €500,000 in new security systems.

[16] Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"

Figure 2.5 Average detection and escalation costs per organisation '$



Response cost and cost of securing network

The response to a data breach is critical to ensuring that this does not happen again, but more importantly reassuring stakeholders that such a breach cannot happen again. In this regard the reputation of a company is critical. The costs of such a breach can be as high as $1.4 million[17].

Figure 2.6 Average ex post response costs per organisation '$

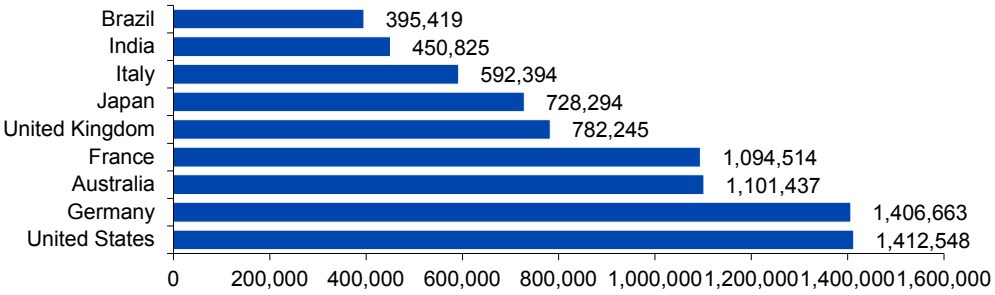
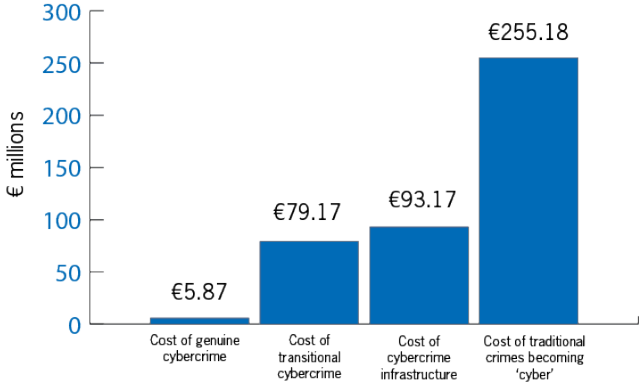


Figure 2.7 - Costs of cybercrime



[17] Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"

Indirect losses

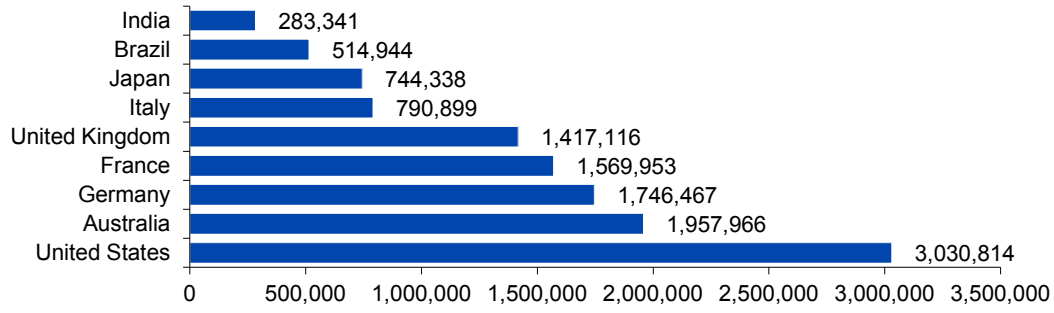
For companies that suffer a data breach there are less direct and intangible lost business costs associated with such an incident. These include abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

Factors influencing the cost to businesses of a data breach

1. the company has an incident management plan.
2. the company had a strong security posture at the time of the incident.
3. Chief Information Security Officer appointed.
4. data was lost due to a third party vendor.
5. company notified breach victim quickly.
6. the data breach involved a lost or stolen device.
7. consultants were engaged to help remediate the data breach.

A company's reputation can be difficult to quantify, however its importance cannot be underestimated. It is only when it is damaged one truly sees its value. The loss of confidence in the brand and associated goodwill can have devastating impact on the share price of a company. The Poneman Institute have estimated that average lost business costs could be as high as €3.03 million[18].

Figure 2.8 Average lost business costs per organisation, '$



Cost of cybercrime to Ireland

In addition to the costs to individual businesses there is the larger cost to the economy of Ireland itself.
To estimate this figure we have built upon the framework of University of Cambridge in the paper "Measuring the Cost of Cybercrime" and applied it to the Irish economy. This framework estimates the global costs of the individual elements of cybercrime and scales these estimates to the country using its share of global GDP. Following this rationale, we have estimated the cost of cybercrime to the Irish economy to be circa €630 million. The analysis, shown in the Table 2.2, highlights that it is the cost of traditional crimes moving online that is the greatest threat to the Irish economy. This cost includes welfare fraud, tax fraud and tax filing fraud.

For the new types of computer crime, it is the defence and indirect costs that are in fact the most significant element and not the direct costs as one may assume. This could indicate that we should in fact be spending less on the anticipation of such and more in response to cybercrime.

[18] Ponemon Institute, 2013, "2013 Cost of Data Breach Study: Global Analysis"

Table 2.2 – the cost of cybercrime (Ireland, UK, US and Global)

Costs of genuine cybercrime	Irish Est.	UK Est.	US Est.	Global
Share of world GDP	0.23%	2.77%	18.82%	100%
Cost of genuine cybercrime	**€'m**	**€'m**	**€'m**	**€'m**
Online banking fraud				
• phishing	€2.55	€30.75	€208.90	€1,110 [19]
• malware (consumers)	€0.12	€1.44	€9.79	€52
• malware (businesses)	€0.51	€6.15	€41.78	€222
• bank tech countermeasures	€1.70	€20.50	€139.27	€740
Fake antivirus	€0.17	€1.99	€13.55	€72
Copyright-infringing software	€144.00[20]	€1,299.57	€8,829.59	€46,916[21]
Copyright-infringing Music	€20.00 [22]	€92.24	€626.71	€3,330[23]
Patent infringing pharmaceuticals[24]	€31.82	€33	€296.92	€1,578
Stranded traveller scam	€0.02	€0.19	€1.32	€7
Fake escrow scam	€0.34	€4.10	€27.85	€148
Advance fraud	€1.70	€20.50	€139.27	€740
	€202.93	€1,510.32	€10,334.94	€54,915
Cost of transitional cybercrime				
Online payment card fraud	€6.80	€86.09	€584.93	€3,108
Offline payment card fraud				
• domestic	€3.57	€43.05	€292.46	€1,554
• international	€5.00	€60.28	€409.52	€2,176
• bank/merchant defence costs	€4.08	€49.20	€334.24	€1,776
Indirect costs of payment fraud				
• loss of confidence (consumers)	€17.02	€204.98	€1,392.68	€7,400
• loss of confidence (merchants)	€34.04	€409.96	€2,785.36	€14,800
PABX fraud	€8.44	€101.66	€690.69	€3,670
	€78.96	€955.21	€6,489.89	€34,484
Cost of cybercrime infrastructure				
Expenditure on antivirus	€5.79	€69.69	€473.51	€2,516
Cost to industry of patching	€1.70	€20.50	€139.27	€740
ISP clean-up expenditures	€0.07	€0.83	€5.65	€30
Cost to users of clean-up	€68.08	€819.92	€5,570.72	€29,600
Defence costs of firms generally	€17.02	€204.98	€1,392.68	€7,400
Expenditure on law enforcement	€0.68	€8.20	€55.71	€296
	€93.34	€1,124.12	€7,637.53	€40,582
Costs of traditional crimes becoming "cyber"				
Welfare fraud	€34.04	€409.96	€2,785.36	€14,800
Tax fraud	€212.75	€2,562.25	€17,408.50	€92,500
Tax filing fraud	€8.85	€106.59	€724.19	€3,848
	€255.64	€3,078.80	€20,918.05	€111,148
	€630.88	**€6,668.45**	**€45,380.42**	**€241,129**

Note: unless otherwise referenced the source of information is Anderson et al, 2012 "Measuring the Cost of Cybercrime", WEIS 2012

[19] RSA, EMC2, 2013,"Phishing kits – the same wolf just a different sheep's clothing"
[20] BSA, 2012 "Shadow market 2011 BSA global software piracy study", Ninth edition
[21] BSA, 2012 "Shadow market 2011 BSA global software piracy study", Ninth edition
[22] Noel Baker, 2010, "Online piracy 'will cost music industry millions'", 12 October, Irish Examiner. Available at: www.irishexaminer.com
[23] IFPI, 2006, "The recording industry 2006 piracy report"
[24] Ireland, UK, and World – Grant Thornton estimates based on operation Pangea 2013 results.

Social costs

Although this paper focuses on the more financial elements of cybercrime, there are real social costs to an economy and to the welfare of its citizens. Although these costs are inherently difficult to quantify they are important and need to be acknowledged. From our research of the issue we have identified eight key social costs. These are:

1. pace of innovation slowed;
2. victimisation costs;
3. crime prevention;
4. changes in human behaviour;
5. cost of criminal justice for prosecution;
6. cost of over insurance;
7. job losses; and
8. access to illicit materials such as:
    - pornography; and
    - avocation of terrorism.

The importance of cyber security

A safe and secure online environment enhances trust, confidence and contributes to a stable and productive economy both domestically and internationally. This is particularly important for an open, technology focused country like Ireland. The emerging trend of cybercrime and the associated costs to business, consumers and government clearly demonstrate the need to have a clear strategy to deal with the many complex, multifaceted and evolving issues.

A strong cyber security strategy is becoming a prerequisite for both the private and public sectors. However, despite this most organisations and governments are extremely inefficient at fighting cybercrime.

The private sector continues to build capabilities in data security and operate the day to day management of cybercrime, but the public sector needs to support these efforts by ensuring that strong regulatory and enforcement frameworks are in place.

Principles for cyber security

Ultimately the same principles of security that exist in the physical world must be present in the digital and as such should protect the fundamental rights of expression, personal data and privacy. To assist with the development of national legislation on the issue of cybercrime, the OECD has developed seven principles governing the protection of personal data including a strong focus on security. These are illustrated by Figure 2.9.

F

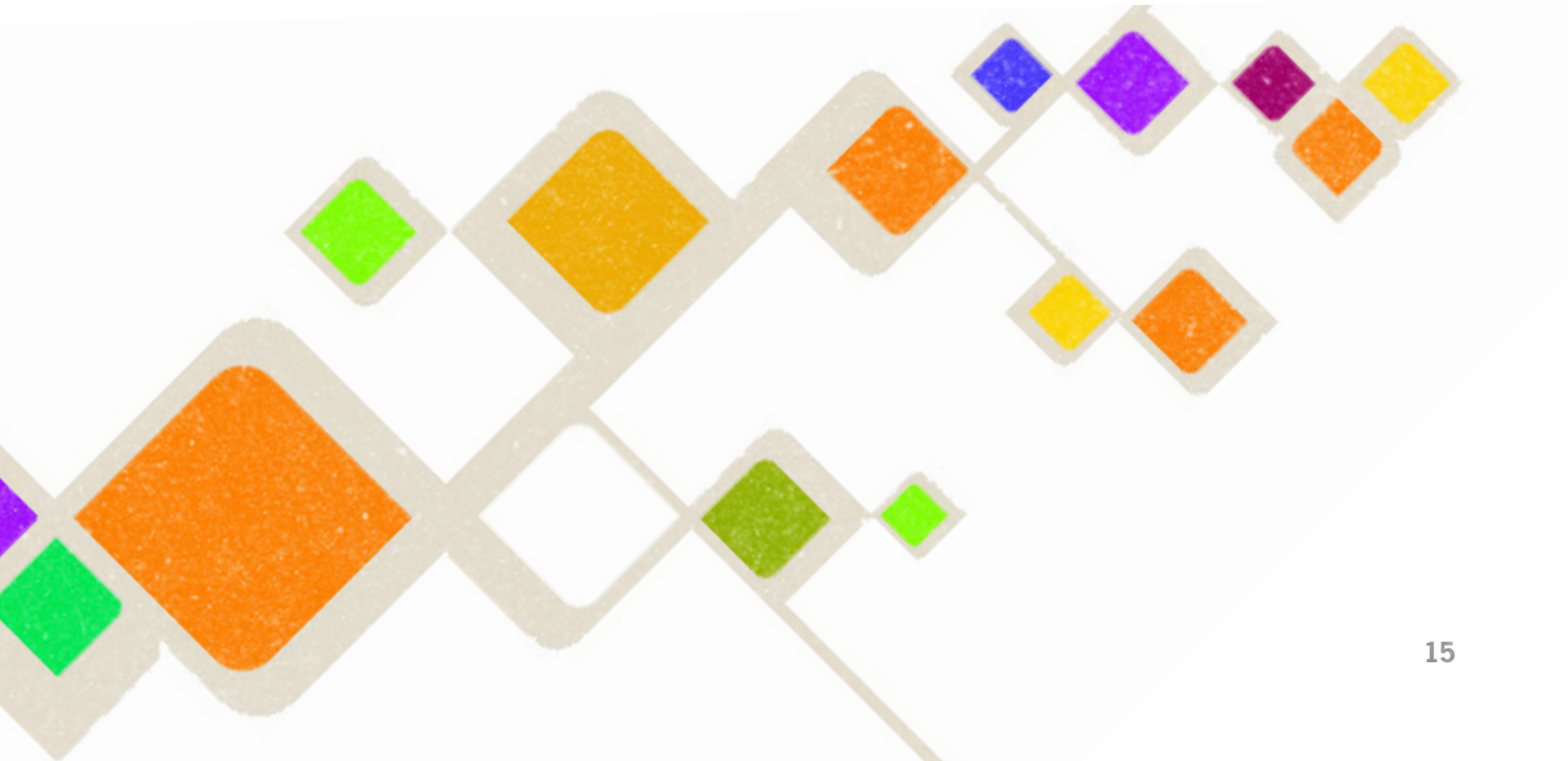
To achieve appropriate level of protection of data it is vital that strategies are developed that build upon these principles whilst ensuring that they:

- leverage public-private partnerships and build upon existing initiatives and resource commitments;
- reflect the borderless, interconnected and global nature of today's cyber environment;
- adapt rapidly to emerging threats, technologies, and business models.
- are built on a risk-based approach;
- focus on awareness; and
- focus on current cybercrime threats.

Key trends affecting cyber security in Ireland

Grant Thornton's experience shows that security controls on IP in Irish organisations are generally poor and remedies in law are rather restricted. Key issues include:

1. absence of document management means that organisations often do not know what IP is in their possession;
2. loose technical and process controls make it straightforward to steal information, and difficult to investigate such thefts;
3. lack of awareness of IP theft in the Irish business community leaves many organisations exposed to IP loss, and means that much IP theft is never detected;
4. cultural factors make it easier for employees to rationalise IP theft than financial fraud (e.g. "I'm only copying my own work, I'm not destroying it");
5. training on IT security and cybercrime prevention in Irish organisations is rare to non-existent;
6. weak laws and police underfunding have historically made it difficult to get IP theft prosecuted, although this is changing; and
7. civil remedies, while available, are typically expensive.



The legislative challenge

Legislating for cybercrime remains a challenge for law makers across the world. The current approach, which has evolved from the traditional or real world criminal and intellectual property law, is not sufficient to tackle the complexity and dynamic nature of the digital world.

It is the delay between the recognition of potential abuses of new technologies and the necessary amendments to national and international law that remains the most significant challenge in this regard. A further challenge is the multi-jurisdictional nature of cybercrime, which makes it difficult for organisations to comply with the many different and sometimes contradictory laws across its various locations. The burden of compliance can be high. In this section we outline the main laws and policies surrounding data protection in Ireland, Europe and the broader international community.

International co-operation

Cybercrime laws across the international community remain largely inconsistent or incompatible which has resulted in slow progress on international harmonisation, which is extremely important in the fight against cybercrime.

To assist the companies and governments operating in the changing digital landscape, efforts have been made to promote co-operation, both nationally and internationally between agencies. This is done through the various international initiatives to facilitate this co-operation, which includes:

- UN General Resolution on cyber security;
- G8; and
- OECD.

Fundamentally, the investigation and prosecution of cybercrime presents a number of challenges for both sides of the law - regulators and enforcement agencies. Whilst there are a number of various forums and international best practice guides, the legislation in place is not adequate to meet the changing demands of the cyber security landscape. The legislation that does exist varies significantly. As a starting point, adjustments to national laws must begin with the recognition of the abuse of new technologies, which could be assisted by mandatory international data breach notifications.

Europe

European law is built upon the principles of the OECD recommendation from Figure 2.9. The EU issued a Data Protection Directive (95/46/EC) in 1995 which covers the processing and security of personal identifiable information. The notable absence within this directive was a general breach notification requirement.
The introduction of such a requirement has been the subject of much debate, which has resulted in the publication of its proposal for a regulation on the protection of individuals with regard to the processing of personal data and the movement of such data. It is intended that the regulation would replace the Data Protection Directive and that would remove the need for EU harmonisation of minimum standards.

The main cybercrime laws and regulations in the European Union

- **European Communities (Electronic Communications Networks and Services)**
- **Data Protection Directive (95/46/EC)**
- **Proposed Directive (~2015)**

Frameworks and forums to aid harmonisation

- **2005 Council Framework Decision on attacks against information systems**
- **Cybercrime Network Conference**
- **European Cybercrime Centre (Jan 2013)**
- **Budapest Convention**
- **2005 EU Framework**
- **EU Cyber Security Strategy**
- **Cybercrime Network Conference**
- **European Cybercrime Centre (Jan 2013)**
- **Budapest Cyber Convention**

Ireland

With no general breach notification in the EU, Ireland itself has adopted a voluntary breach notification Guidance and Personal Data Security Breach Code of Practice ("the Code").

However, the Code is not legally binding. In addition to the Code, there are also the regulations which apply to certain entities in the telecommunications sector.

Under the Code, the data controller of a business must immediately consider whether to notify the affected data subjects in situations where personal data has been put at a risk of unauthorised disclosure, loss, destruction or alternation.

In Ireland, whilst we have legislation and guidelines in line with other countries, legislative gaps still remain. In particular, the 2005 EU Framework Decision on attacks against information systems has not been transposed into Irish law.

This would give effect to the Cybercrime Convention, as referred to already. Until implementation of the Cybercrime Convention and transposition of the Council Framework Decision on attacks on information systems into domestic Irish law, national law enforcement agencies across the Cybercrime Convention signatories, including Ireland, can only combat the more complex and generally international computer crime within the boundaries of limited domestic laws.

The main data protection laws and regulations in Ireland

- **Personal Data Security Breach Code of Practice (the "Code");**
- **European Communities (Electronic Communications Networks and Services);**
- **(Privacy and Electronic Communications) Regulations 2011 (the "Regulations);**
- **Data Protection Acts 1988 and 2003; and**
- **Proposed Criminal Justice Bill.**

Conclusions

To say that cybercrime is an epidemic is not accurate. This would imply that organisations could avoid being compromised through good IT security hygiene or responsible investment. This is increasingly not true. For the vast majority, including those in Ireland, the question is no longer if they will be a victim of cybercrime but when?

The scope of compromises is rapidly increasing and the amount of data stolen on a daily basis is truly alarming. Some companies have lost all intellectual property related to the design of high-tech technologies and others have had millions of euros stolen from their accounts in a matter of days. The public will not always read the details of these cases because disclosure is not mandatory, but it is clearly a serious problem.

Key findings

- while it is difficult to quantify, we estimate cybercrime is costing the Irish economy circa €400 million per annum. This is in line with international estimates;
- the research indicates we may be spending too much on prevention of cybercrime and not enough on reacting to it when it happens;
- "big data" technologies are increasing the effectiveness of cybercrime attacks;
- organised criminals continue to be the drivers of cybercrime;
- financial motives continue to be at the heart of the increase in cybercrime; and
- non-reporting of cybercrime by business and individuals continues to be an issue both in Ireland and globally.

Key recommendations

Cybercrime is heavily impacting on the economy, both in Ireland and internationally. Its international nature makes it difficult to prevent particularly in a small open economy like Ireland. It is, however, critically important for Ireland to lead in the international fight against cybercrime. Ireland's fast growing technology sector is a key driver in our economy. Our government needs to legislate appropriately, businesses need to detect and prevent cyber-attacks and our work force needs to be aware of and have the skills to fight cybercrime and secure online systems. Only with this combination can Ireland protect its businesses and consumers in the online world and protect technology and intellectual property driven foreign investment. More specifically:

- Ireland needs help to ensure international harmonisation of cybercrime laws. In particular, Ireland should implement the 2005 EU Framework Decision on attacks against information systems including mandatory data breach disclosure;
- Ireland should urgently develop and publish a national cyber security strategy. This is a plan designed to improve the security and resilience of Irish national infrastructures and services. It should establish a range of national cyber security objectives and priorities to be achieved in specific timeframes;
- Irish businesses 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 subjected to an online attack but a question of when? The ability of the business to detect and react to the attack will be the key factor in limiting the impact of the cybercrime; and
- ensuring appropriate education of the impact of cybercrime on Ireland is key.

This includes ensuring:

- consumers understand the basics of protecting themselves online;
- business leaders understand the impact of cybercrime on their businesses. There have been a number of government initiatives in the UK that could be mirrored (e.g. the FTSE 350 Cyber Governance Health Check); and
- in addition, whilst there are a number of courses in our third level institutions that address cybercrime and security issues, these subjects need to be expanded in the undergraduate syllabus and ensure that all technology graduates are aware of cybercrime, its impact and security techniques to prevent it.

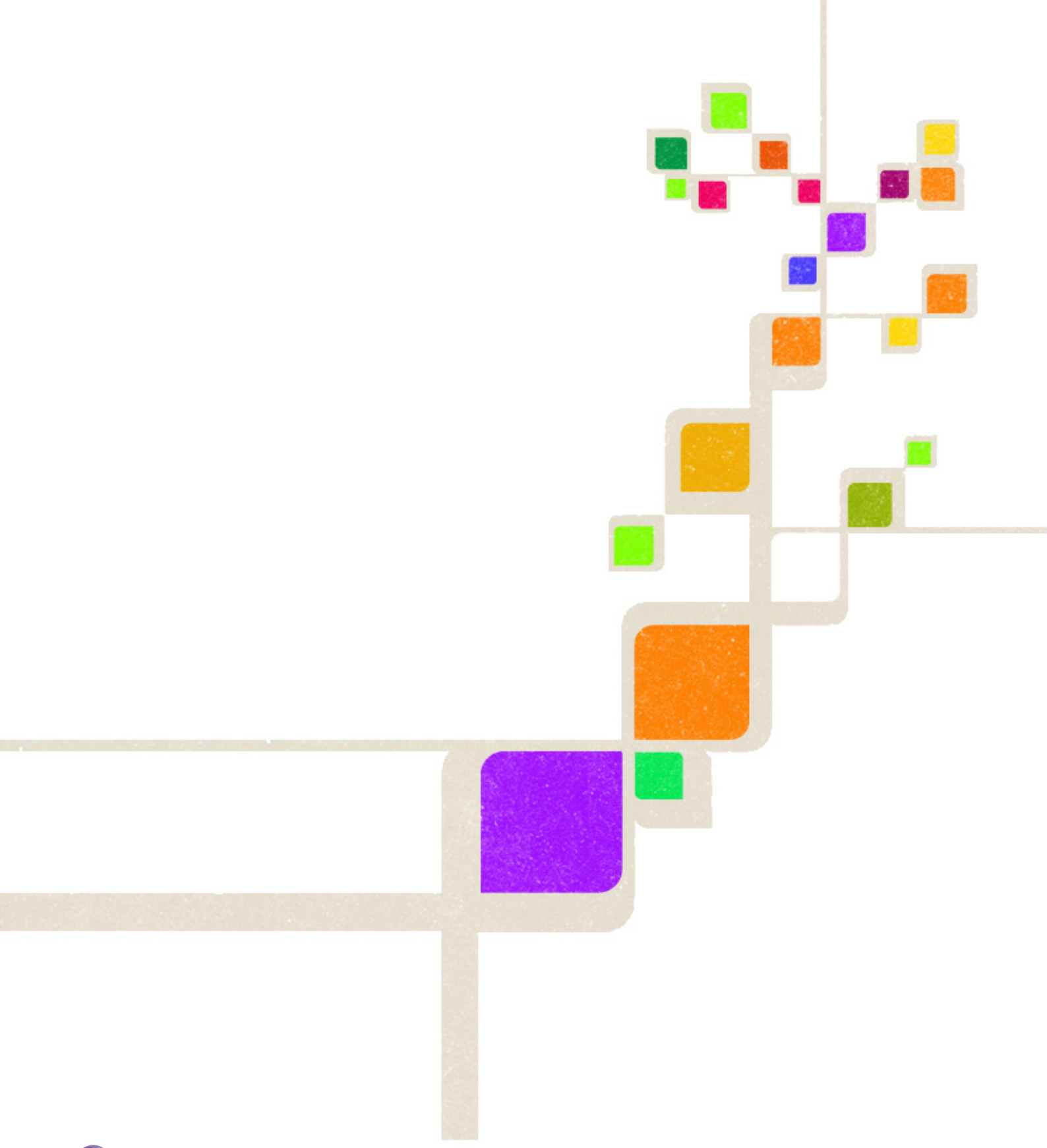
Contacts

Mike Harris
Partner
T +44 (0)28 9587 1071
E mike.harris@ie.gt.com

@GrantThorntonNI

www.grantthorntonni.com

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



Grant Thornton

An instinct for growth™