Deloitte.

Cyber opportunity analysis report 2016
Positioned to lead
...by building on existing strengths in the technology sector, in addition to a growing cyber cluster, Ireland is uniquely placed to benefit from increased global investment with a real opportunity to position itself as a world class cyber security practices, solutions, and investment hub.
Introduction

The World Economic Forum in Davos identified cyber related threats as one of the highest of all global risks in terms of impact of events and likelihood of events occurring. The global IT research and advisory firm Gartner estimates that global IT security spending will grow to US$76.9 billion in 2015 with a flood of investment expected in companies that provide cyber security software, solutions, and services including R&D investment.

Data breaches are becoming bigger and more common. Over the past twelve months there have been many high profile cases reported involving household names in Ireland and international corporations such as Sony, Ashley Madison, JP Morgan, TalkTalk to name but a few. This is a pervasive issue. According to the Irish Computer Society (Jan 2015) over 50% of Irish companies say they have suffered a data breach over the past year. The figures may be even higher as companies are often reluctant to admit a data breach for fear of negative publicity.

Furthermore, regulators are struggling to deal with the pace of technological change. Balancing the rights of individuals to privacy with the growth of online services that require personal data has become a thorny issue. This has been highlighted by the recent case against Facebook, which has been taken to the European Court of Justice and the suspension of the EU Safe Harbour agreement.

Consequently the costs for businesses are enormous. It has been estimated that spending on information security will grow from its current level of circa US$75bn to over US$150bn by 2020 leading to a rapid growth in the cyber security sector worldwide. New specialist companies are being set up at a rapid pace to provide solutions and services in this growing sector. Undoubtedly it will provide significant opportunities for businesses, and the countries in which they operate.

By building on existing strengths in the technology sector, in addition to a growing cyber cluster, Ireland is uniquely placed to benefit from increased global investment, and has a real opportunity to position itself as a world class cyber security practices, solutions, and investment hub. The large number of global high tech and financial services organisations already represented in Ireland provides a level of ‘critical mass’ for investment, skills development, and operations throughout Europe.

As such it is felt that there is significant potential for Ireland to develop a cyber cluster and become a global leader in this increasingly important area. In order to explore how this potential can be best capitalised on, Deloitte, in association with the International Sustainability and Investment Centre, carried out its inaugural opportunity analysis for Ireland in the area of cyber security. This high level analysis assessed the potential for Ireland and highlights the potential steps that could be taken to ensure that the economic benefits in terms of job creation and investment can be realised.

In preparing this analysis Deloitte carried out a survey of senior industry executives and public servants and conducted various follow up interviews in order to get their perspective on:

- Key cyber security trends
- Important factors for cyber security businesses in deciding where to locate
- Top locations globally for cyber security businesses
- The relative merits of Ireland as a base for cyber security businesses

Ireland has a real opportunity to be at the forefront of cyber security. It has long proven itself to be an innovative technology hub, and this is another area in which it can become a global leader.
This analysis was conducted during the summer of 2015 with over 70 responding to the questionnaire and taking part in interviews. The respondents were primarily senior executives in various industries most notably the technology & financial services industry and senior public servants.

**Fig. 1 Primary function of the respondents organisation**

- 35% Real Estate
- 17% Consumer Business
- 8% Financial Services
- 7% Public Sector
- 19% TMT
- 13% Energy and Resources
- 8% Other
- 1% Other

**Fig. 2 Primary title of respondent**

- 30% Managing Director/Chief Executive Officer
- 21% Chief Financial Officer
- 21% Chief Information Officer/Head of IT
- 15% Chief Information Security Officer/Information Security Professional
- 15% Partner/Chairman/Member of the Board
- 15% Other Senior Management
- 1% Other
Cyber Security Trends

The number one trend emerging from the analysis is “Increased regulation on Data Privacy” which was mentioned by nearly three quarters (73%) of respondents. Ever since the revelations by Edward Snowden in 2013 about the US National Security Agency’s surveillance programme this has become a sensitive and controversial issue.

At present there is a patchwork of laws and regulations in different countries. As more personal data is stored by organisations and with the growing threat of terrorism there is a need for transnational cooperation. However cultural differences in attitudes to privacy make this problematic. In Europe privacy is considered to be a fundamental right of citizens whereas in the US, privacy is considered more in terms of consumer protection. This cultural difference was highlighted recently in the case against Facebook brought by Austrian student, Max Schrems.

In the late 1990s, the US and the EU put in place a “safe harbour” pact which allowed firms to export data if certain safeguards were provided. This pact was struck down by the European Court of Justice in October 2015 following the case taken by Schrems. It’s not yet clear what will emerge from the wreckage. The European Commission is currently in the process of updating its Data Privacy Directive.

What is clear is that organisations will need to keep on top of the changes in regulations and put in place controls and processes to ensure compliance.

Cybercrime

Perhaps unsurprisingly the growth in cyber crime featured highly as a trending concern. 59% of respondents cited “more sophisticated scams” and 53% cited “growth in identity theft” as major trends. Cyber attacks take a number of different forms but broadly fall into two major categories.

PHISHING
Where an attacker collects user credentials, passwords, credit card details using fake emails and text messages that appear to be genuine.

MALWARE
Where viruses, worms, trojan horses, spyware, are uploaded onto PCs or networks without the knowledge of the user to disrupt computer operations or to gather sensitive information. Malware can go undetected for months, with some variants of malware undetected for years.
A recent estimate by the Centre for Strategic Studies puts the annual global cost of digital crime and IP theft at US$445 billion! Cyber crimes often involve multiple jurisdictions which makes investigations time-consuming and complicated. Securing cyberspace is difficult because the architecture of the internet was designed to promote connectivity rather than security.

In our view cybercrime is only going to grow. Online retailing (etailing) and online payments are growing rapidly. Most estimates suggest that ecommerce will double over the next five years. In addition billions of new devices (such as cars, fridges, heating & lighting systems, medical devices) will become connected to the web leading to the term “Internet of Things (IoT)”. Cisco Systems estimates that by 2020 over 50 billion “things” will become connected to the internet which will further increase the scope for cybercrime.

Organisations are responding through employee education programmes, investing in better encryption, biometrics and insurance protection. It all comes at a cost. Gartner estimates that nearly US$70 billion was spent in 2014 by organisations on data/information security.

Specialisation

The third major theme evident from the analysis is that businesses will change how they organise and manage data security either internally or through third party providers. 36% of respondents felt there would be a trend towards outsourcing cyber management to third party organisations and nearly 27% think that businesses will establish global/regional centres of excellence for managing this function.

In our view the implication of this trend is that a small number of locations will be preferred for establishing centres of excellence in the same way that certain locations became favoured for establishing Shared Service Centres. The factors which are most important for locating cyber businesses are dealt with in the next section of this report.
Best locations for cyber businesses and rationale

Specialised skills

We asked respondents to identify the key factors for deciding where to locate a cyber business. An overwhelming number of responses were skills related. In fact the top three responses were all related to skills.

- **87%** of respondents identified access to specialised skills as a top factor.
- **56%** mentioned a cluster effect; i.e., the number of similar/related businesses in the area.
- **54%** noted the quality and number of skilled graduates/post-graduates.

This is not surprising as there is currently a significant talent shortage globally within the technology sector. The technology sector is booming particularly in fields such as cloud computing, data analytics, mobile technologies and information security. According to the ICT Skills Report by the Department of Jobs, Enterprise and Innovation there is a shortage of over 800,000 ICT professionals across the EU. More than 200,000 cyber security jobs in the US are unfilled, and postings are up 74% over the past five years, according to Peninsula Press (a project of Stanford University Journalism Program in California). Demand for cyber security professionals over the past five years grew about 12 times faster than for all other jobs, according to a report by Burning Glass Technologies in Boston. So this trend is unlikely to change anytime soon.

Fig 4. Top factors for companies in locating cyber business

- **Access to specialised skills** (87%)
- **Cluster effect** (56%)
- **Quality and number of skilled graduates/post-graduates** (54%)
- **Ease of doing business** (46%)
- **Linkages of major universities/research centres** (41%)
- **Taxation environment** (36%)
- **Neutrality of jurisdiction** (36%)
- **Government incentives (grant/incubation centres etc)** (31%)
- **Access to capital** (23%)
- **Stringent laws governing intellectual property rights** (17%)
- **Extensions spin-offs existing technology providers to cyber space** (13%)
- **Extensions spin-offs of exiting FSI providers to cyber space** (3%)

Business environment

After skills the next broad location factor deemed important for cyber security businesses is the business environment.

- **46%** of respondents mentioned “ease of doing business” as a key location factor. Presumably this refers to factors such as absence of red tape; ease in obtaining work permits for foreign employees; availability of suitable property; quality of infrastructure and transport linkages.
- **Taxation environment (36%) and availability of government incentives/grants (31%)** also featured highly.
- **Finally jurisdiction neutrality (36%) and the quality of the legal system governing Intellectual Property rights (17%)** were also deemed important. Clearly cyber businesses are concerned about protecting their IP and knowledge from Government snooping and corporate theft.

Linkages to major universities and research centres

The quality of research universities in the vicinity is clearly important too (41%). The cyber sector tends to be at the leading edge of technology development so establishing linkages and collaboration with universities is important to cyber businesses. Collaboration can generate spin-off opportunities and provide access to an additional talent stream.
Top locations

USA - The number one location for basing a cyber business according to the participants is, by a distance, the US. Over 35% ranked it as the top location and over 60% ranked it in their top 3. The main reasons cited for this ranking were availability of skills and linkages to the technology sector (Silicon Valley being the centre of the technology universe). Access to venture capital funding and the strength of IP laws were also mentioned.

UK - The clear second choice according to respondents is the UK. Over 60% of respondents ranked it in their top 3. In addition to availability of skills and industry linkages participants mentioned its location and the level of government support the industry gets.

After the US and UK there were 5 locations that got credible mentions. Ireland, Israel, Canada, Australia and India. For Ireland the key reasons cited were the quality of the workforce and education system, its technology footprint and its location in the heart of the EU. For Israel the extent of government support and military involvement were key factors as well as its strong reputation in the industry.

In South America, Brazil was seen as the best location for cyber business.

It is notable from the responses that in Europe, apart from the UK and Ireland, hardly any other jurisdictions featured.

All respondents to the survey are based in Ireland, and so it must be borne in mind that a natural bias towards Ireland may skew results slightly.

Fig 5. What are the current locations/jurisdictions of choice for cyber security businesses?

Fig 6. Reasons for ranking specific locations
Ireland as a location for cyber security businesses

We can see from the previous section that Ireland was ranked highly as a location for basing a cyber security business. We asked respondents to give their views on Ireland’s relative merits as a location for basing cyber security businesses. The responses are interesting as many factors were highlighted as being both a positive and negative factor as can be seen from the analysis below.

Fig 7. How would you rate Ireland as a base for cyber security?

Skills - the number one factor:

Skills came top of the list for both positive (50% of respondents) and negative (34% of respondents) factors. Digging a little deeper it would appear that Ireland has a reasonably sized pool of technology talent and that our education system is well regarded. This is borne out of the IMD World Competitiveness Yearbook, which benchmarks 60 countries across a number of key areas for Foreign Direct Investment. In its 2014 yearbook Ireland was ranked 1st for both the availability of skilled labour and for its workforce flexibility and adaptability.

However it appears that the depth of the talent pool for cyber businesses is moderate. Essentially, there does not appear to be enough of the specific skills to satisfy demand. As discussed in the previous section, this is a global issue, and not specific to Ireland. The Department of Jobs, Enterprise & Innovation has recognised this limitation and has developed a comprehensive action plan to remediate the situation. Graduate enrolments in science, maths and computing courses have increased dramatically over the past five years and now stand at more than 30,000 annually. This bodes well for the future however inevitably there will be a time lag before the graduates come on stream as skilled cyber professionals.

Technology footprint

The second most positive factor mentioned by respondents is “proximity to industry” (25% of respondents). This is presumably due to the scale of the technology footprint in Ireland - many of the leading global technology companies have a significant presence here. The infographic below illustrates Ireland’s technological footprint.
In addition to having a technology cluster, approximately 10% of the Top 500 cyber companies have a presence in Ireland, with three Irish companies now featuring in the Top 500.

Other positives

Some other positive factors which were mentioned include Ireland’s location (and a member of the EU); the fact that we speak English, which has become the de facto language for the technology sector; we are “business friendly” including our corporation tax regime - although this was not as significant a factor as one might think.

Not all positive - some areas where we could do better

In addition to depth of the talent pool there were some other negative factors mentioned including access to capital/funding (17% of respondents); the cost base - Ireland is seen as a relatively expensive location; and government policy. A number of respondents (17%) are of the view that the Government isn’t doing enough to develop and promote the cyber business sector.
The Deloitte Cyber Security Opportunity Analysis is high level. Nonetheless it generated some interesting findings:

1. **Cyber security** is a sector which is **going to grow rapidly** for a number of reasons
   - the continued growth of ecommerce using fixed and mobile devices
   - increasing levels and sophistication of cybercrime
   - the growing threat of terrorism in the developed world
   - the increasing number of “things” that are becoming connected to the web

2. **Data security** will increasingly be **managed by specialist units** on a captive (centres of excellence) or outsourced basis

3. Companies will need to **tread carefully in handling and securing data** as Regulators try to navigate the inherent conflict between personal privacy and data storage/usage.

4. The **US is currently the number one location for cyber business** by a comfortable margin.

5. **Ireland ranked reasonably well** in its relative attractiveness as a location for cyber business. However its cyber footprint is small and there is scope for further action and development. The good news is that there appears to be no dominant jurisdiction for FDI so it’s all to play for.

---

**Conclusion**

**Realising the Opportunity**

As we emerge from the most severe recession in recent decades, Ireland is experiencing a positive growth in economic activity. Over the past five years, the foundations for this growth have been largely driven by successful collaboration between the State, agencies and local / foreign owned enterprises by means of targeted initiatives. Combined these have enhanced Irish competitiveness while leading to increased job creation across the whole economy.

The government’s most recent Action Plan for Jobs 2016, sets out an ambitious plan to build on this success by continuing to support the development of a new, sustainable economy based on three pillars of enterprise, exports and innovation.

**Cyber security cluster development**

A key component of the Action Plan for Jobs 2016 is the continued support for existing economic sector clusters, while at the same time identifying new areas of cluster opportunity under the new ‘National Clustering initiative’. This initiative aims to identify new areas of economic opportunity and build out additional clusters of scale and international visibility in areas of strength.

As is evident from our cyber opportunity analysis, cyber is one such new area of opportunity that at a global level we are well positioned to lead.

From this analysis, Ireland is uniquely placed to benefit from increased levels of global cyber investment, and has a real opportunity to position itself as a world class cyber security practice, solutions and investment hub underpinned by meaningful research activities and test-bed facilities.

**Growth potential**

With a growing cyber sector in Ireland, as a country we can accelerate this growth by leveraging off existing strengths that includes our technology and financial services sectors footprint, supportive business environment and high degree of talent mix.

Communicated effectively, these factors can be used to further attract investment, skills development and operational hubs for wider EMEA activities, while at the same time supporting the development of local Irish owned companies that will drive export led growth.

**Cluster of scale and international visibility**

The opportunity for Ireland to position itself as a leading global cyber security hub does exist. Across government, enterprise and academia, considerable assets that can help achieve this ambition are already in place. These have been built out at considerable expense over the last number of years, as such can be leveraged off thereby minimising any potential cost of developing Ireland as a cyber hub.

That said, while recognising and leveraging off existing strengths is an important first step, our opportunity analysis also noted areas of concern that could act as potential blockers to realisation of ambition. These included further skills development, access to capital and overall Irish cost base.
Proposed next steps

Internationally Ireland is recognised for its success in developing economic clusters of scale in areas such as IFS, MedTech, ICT and Pharma among various clusters. In the past, a major success factor in such cluster development has been the collaboration between the State, agencies and enterprise stakeholders working together to create enabling frameworks for specific clusters to flourish.

While we hope to explore some of the themes highlighted by this initial opportunity analysis in greater depth in future research and analysis, our view is that there are a number of key actions that could be taken now to capitalise on this opportunity. In order to position Ireland to realise a cyber hub opportunity, a collaborative approach is a fundamental requirement, therefore it is suggested that a Working Group of public and private sector stakeholders be established to further explore this opportunity.

Potential areas that could be reviewed or explored in future in depth analysis include:

» **Education and training to meet the industry needs.** Support third level institutions in Ireland in rolling out cyber security courses across the island of Ireland and build on the success of some of Ireland’s leading third-level institutions offering cyber specific courses. Areas for possible consideration include enhancing the ICT Action plan to include a high-level action plan for cyber skills. Working in conjunction with industry, third-level institutions could also provide conversion courses to fast-track honors-level graduates from other disciplines into specialist cyber security courses.

In addition to the inclusion of cyber on the agenda of third-level instructions, Ireland should also explore the benefits and feasibility of including cyber on the second-level curriculum. Focusing on preparing students from a young age and exposing them to key skills required in cyber could prove to be a significant long term benefit to meet Ireland’s ever-growing demand for cyber talent.

» **Start-up and Incubation Facilities.** Explore the possibility of leveraging off existing national incubation facilities for start-ups to support those interested in developing cyber products or setting up cyber security practices and solutions. Additionally, research and development centres could be created focusing on the development of innovative cyber security solutions.

» **Access to Capital.** Assess the feasibility of existing and/or develop new investment platforms to support Ireland’s growing cluster of cyber enterprise, including but not limited to seed, venture capital and private equity.

» **Promote Ireland.** Leverage off excellent existing public and private sector promotional platforms to internationally market Ireland as a location of choice for cyber security practices, solutions and investment.

» **National Cyber Security Strategy.** Implement and further enhance the National Cyber Security Strategy.

Over the next number of years we will see a dramatic increase in the levels of global cyber investment. For Ireland our stated competitive advantages, a growing cyber cluster and a partnership approach combined has the potential to allow Ireland develop as a world class cyber security practice, solutions and investment hub.

In developing such a cyber cluster of scale and international visibility, bringing together an existing asset base with additional supports focused on skills and access to capital, would give Ireland scope to realise this opportunity.
For further information or if you would like to discuss any aspect of the report in more detail please contact:

Colm McDonnell
Partner - Risk Advisory
Deloitte
T: +353 1 417 2348
E: cmcdonnell@deloitte.ie

Camilo do Carmo Pinto
Manager - Cyber Risk Services
Deloitte
T: +353 1 417 2687
E: cdocarmopinto@deloitte.ie

Stephen Nolan
CEO
ISI Centre
T: +353 1 525 0290
stephen.nolan@gifsc.ie

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As one of the largest global professional services and consulting networks, with over 220,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has approximately 2,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience, and insight to collaborate with clients so they can move forward with confidence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2016 Deloitte. All rights reserved