There are close to 50 indigenous companies working in the broad area of information security. Ireland is also home to major security multinationals carrying out high-level work, including McAfee, Symantec, Trend Micro and Microsoft, in addition to more recent arrivals like Mycroft.

“Many job vacancies for experienced information security professionals are going unfilled, Ireland’s computer emergency response team has warned.

“Despite the recession, a lot of infosec roles are not being filled due to lack of talent,” said Brian Honan, head of IRISSCERT, the Irish Reporting and Information Security Service computer emergency response team. He said he is contacted regularly by firms looking for experienced information security professionals capable of putting together security programmes for their organisations.

For example, Amazon’s development centre in Dublin has several open positions for computer security personnel. Pharmaceutical and financial services companies, which are plentiful in Ireland, are just two sectors where protecting information is vital. “They’re either bringing that talent in or they’re hiring here,” said Honan.

He pointed out that one of the Government’s aims for its smart economy strategy is for Ireland to become a preferred location for data centres. “Those will need security skills,” Honan pointed out.

There are places where people can acquire the necessary expertise, he added. Some of the world’s leading IT security software companies operate threat centres in Ireland, including Symantec, Microsoft, and Trend Micro, while McAfee has a sizeable operation in Ireland. “There are vacancies, a career path and opportunities for people with the right skills,” said Honan.

Ref: www.siliconrepublic.com/strategy/item/18903-skills-deficit-leaving-it-s

Worldwide there are about 1.5 million people working as computer security professionals and employment in this area is growing at approximately 9% per year and industry projections are that this rate of growth will continue or improve in the future.

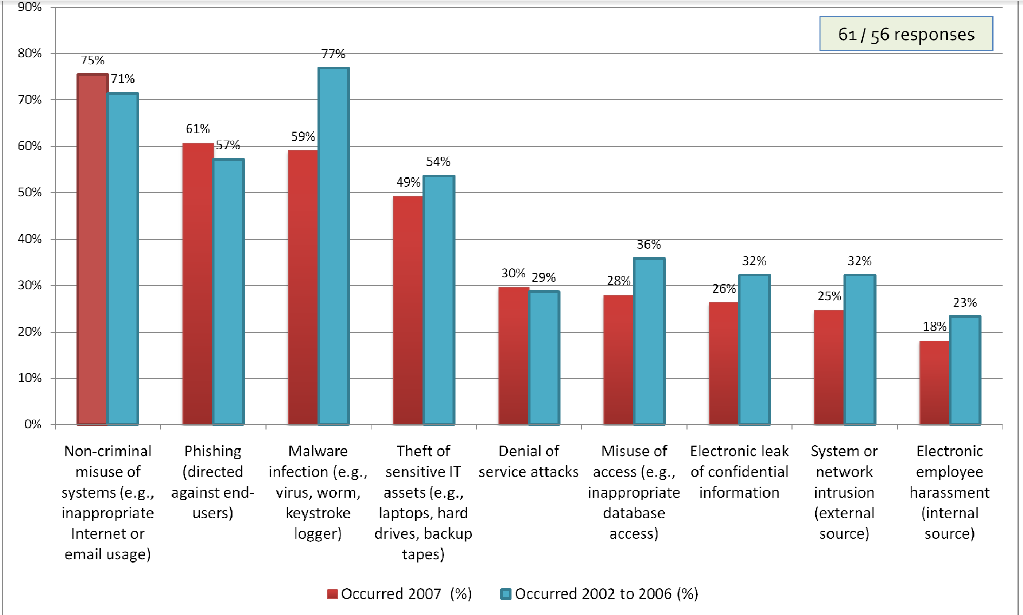
Typical employers in the computer security field include:

* Companies running enterprise computer networks;
* The payment card industry;
* Companies involved in e-commerce;
* Financial services companies;
* Academic institutions;
* Government departments;
* Internet service providers.

Each of these service providers have distinct security needs which require different solutions to meet their needs.

Thus graduates in this field require not only a technical background in general computing but also specialist knowledge of the differing security needs of different types of businesses, the primary technical solutions available to meet these needs, the primary methods of attack on computer systems, how to plan for such attacks both in terms of defense and damage control, how to detect intruders and how to gather evidence to identify the intruders, track their actions and present evidence detailing their activities.

In the last decade, we have witnessed a significant change of emphasis in relation to computer security, network security and secure web services. This has been partially driven by the increasing trend towards web and cloud based services, accompanied by an upward trend in consumer trading on the web. Taking risks with an organisation’s information security may breach legal compliance requirements and lead to an expensive process of litigation. 34% of respondents to the recent ISSA/UCD Irish Cybercrime Survey reported theft of sensitive IT assets, 30% reported denial of service attacks with single incident costs of up to €250,000. Indeed 14% of respondents spent in excess of 10 working weeks responding to individual issues. The following chart taken from the ISSA/UCD survey shows the variety of incidents reported.



The ever present threat associated with internet connectivity and the increasing probability of financial loss due to system compromise has created a need for companies to assess the vulnerability of their computer infrastructure and software to attack.

Companies are now beginning to realise the benefits of simulating real world attacks, by a determined hacker, against IT infrastructures and software. Documenting such proof-of-concept attacks demonstrates infrastructural weaknesses and/or vulnerabilities in software. Terms such as technical networking and systems security, aggressive network attack and self-defence, holistic security are rapidly becoming buzzwords and the need to implement international best practice is now an imperative.

Ensuring that companies have the skills and knowledge necessary to protect business from security threats is critical. Investing to protect information assets makes sound business sense.

Given the current level of attacks on computer systems worldwide and the escalation in security related employment, a niche has been created in the area of system and software security. The proposed course is will impart the skills and knowledge necessary to make informed decisions to enhance corporate governance, mitigate risk and protect information assets.

The department of computing has been in discussions with Pramerica Systems Ireland Ltd, with a view to developing an MSc in System and Software Security. The aim of the MSc programme is to develop a postgraduate skilled in methods of evaluating the security of computer systems, networks and software, capable of simulating attacks, identifying vulnerabilities and planning and implementing countermeasures. From these discussions and other research we feel that the proposed course would offer significant added value to graduates in terms of skill development and employability. It is planned to address the need for security professionals through the mechanism of an MSc degree run on a part time basis over a period of two years.

Analysis of the job market indicates that demand for IT professionals with security related skill sets is increasing. This is particularly true in the UK where organisations failing to safeguard their processes can be prosecuted by the data privacy watchdog, the Information Commissioner’s Office and fined up to £500,000.

## Information Security is the Key Skill of the Future

AUTHOR: KATIE FRANKLIN 27 OCTOBER 2011

It’s official  —  information security is the most important attribute for IT professionals of the future to possess according to the BCS, The Chartered Institute of IT.

Perhaps not surprisingly, given the almost daily announcement of data losses and high profile hacking attacks, the BCS members voted information security as the top skill for tomorrow’s IT professional.

The skill topped a poll run by the BCS ahead of its IT training and professional development summit. At the summit, CIOs from across the UK discussed what skills the IT industry needs in the future and how organisations can prepare by prioritising IT training and professional development now.

The views of such senior IT figures on the relative importance of information security was reinforced by the fact that it gained more than twice the number of votes of any of the other listed attributes. System development, technical strategy and planning, business process management and business change were the next most popular skills.

Adam Thilthorpe, director of professionalism at BCS, said, “The skills needed by an IT professional are continually changing not only to keep pace with technological advances but also to adapt to the changing nature IT plays today in business and society.”

He went on to stress that the continued expansion of online business opportunities drives the need for information security, assurance, and cyber security skills. He said organisations “needed to understand information and have an approach to risk management”.

So the message is clear: whether you’re contemplating your next career move in IT or planning your organisation’s future training requirements, information security should figure prominently at the top of your list!

Ref: http://globalknowledgeblog.com/technology/security/information-security-is-the-key-skill-of-the-future/

The need for additional personnel with high-level IT security skills has also been cited in both the 2011 and 2012 National Skills bulletin:

Research findings indicate that the immediate skills recruitment difficulties being experienced mainly relate to positions requiring high–level ICT Honours Degree (NFQ Level 8) and above. The demand, in terms of positions, is of an order of scale for:

**“ICT – security experts (100):** Internet security and network security models and solutions - certified IT systems, architecture, engineering and management (e.g. Cisco information security systems), firewall configurations administration, authorisation mechanisms. **”**