www.infosecurityireland.org

Survey of InfoSecurity Ireland members

Summer 2016

Introduction and method.

A survey of members of InfoSecurity Ireland was conducted by CIRCA Group Europe Ltd. from 2 June to 23 Sept 2016. The initial survey was distributed to the emails of 229 ISI members through the SurveyMonkey software system on 2 June 2016. Each member received an email in advance from ISI setting out the purpose of the survey and requesting their views. Each email included an embedded link to an on-line survey; there were 28 responses in all (= 12%).

To prompt further responses, a web-link to the survey was set up and this was provided to additional persons in the info-security sector through stakeholders eg development Agencies. This process also began in mid-June; it is not known how many were contacted by the third parties but 16 responses were received. The survey was closed on 23 September 2016. The overall number of responses was therefore 44. The figure after de-duping was 42, of which 35 were companies, 6 were academic institutions and one was a student. The 35 companies comprised 23 Irish and 12 multinationals. The full list of respondent companies is in Table 2.

Table 1: Survey Respondents

Survey	No contacted	No. Responded	%
E-mail survey	229	28	12.2
Survey link (through 3rd parties)	?	16	
	229	44	19.2

Table 2: Organisations Responding to InfoSecurity Survey

Xyea	BH Consulting	CalQRisk
McAfee	StorageCraft Technology	
Linkresq ltd	BAE Systems	Egis Projects Ireland
Presidion	Copperfasten Tech	Aer Lingus
NetFort Technologies Ltd		Securit Consulting
Certification Europe	Threatscape	Bua Cyber Security
Deloitte	Edgescan	Jumly Limited
VigiTrust	ESET Ireland	Solotonltd
UniVirtua Ireland Ltd	Centuri Analytics	Student
HEAT Software	Daon	Athlone IT
Adaptive Mobile Security	Palo Alto Networks	Dublin City University
Espion	Kinesense Ltd	Dublin Inst of Technology
Clean Communications Ltd	TSSG	Trinity College Dublin
eSentire	Sedicii	UCD
EMC	Arup	

Question 1: Principal area of activity. Respondents were first asked about their principal area of activity within the sector. The question was "*Please indicate your principal area(s) of activity (the options specified are the official ISI classifications). The information will enable the mapping of the cybersecurity landscape in Ireland*".

Table 3: Principal area(s) of activity (n = 42)	
Answer Options	**%**
Security and threat management	56.8%
Data security	45.5%
Network security	45.5%
Governance, risk, compliance	38.6%
Application security	38.6%
Endpoint and content security	29.5%
Incident response, forensics and eDiscovery	27.3%
Identity and access management	22.7%
Disaster recovery, Business continuity	18.2%
Other	36.4%

The 'Other' areas of activity specified were:

- Providing network visibility of all activity on the network, with troubleshooting and forensic analysis capabilities and historical tracking
- ISO 27001, ISO 20000, ISO 22301 and Cyber Essentials Accredited Certification Body which covers all of the above at some level
- Telecoms Carrier Network security including Signalling Security
- Critical Information Protection, Data privacy and protection
- Cybersecurity Strategy, ISO 27001, Security Awareness, Cloud Security, Training
- Telecoms Carrier Network security including Signalling Security
- Security for cloud applications
- In the context of Healthcare Informatics
- Identity
- Social Engineering & Penetration testing
- ISO 27000
- Penetration Testing
- Email and messaging security
- Education and Research

Question 2: Training Needs. Respondents were asked "*The training needs below were identified by an ISI/Skillnets working group. Please indicate your training needs*". The question was phrased to indicate both the needs and the lack of need, i.e. each topic could be indicated on a scale from 'definite' need to 'not required'. The responses are in Table 4.

Table 4: Training needs (n = 41)					
Answer Options	**Definite**	**Probable**	**Unlikely**	**Not required**	**Definite + Probable**
Advanced algorithms & data structures	6	4	11	15	10
Advanced threat detection (8)	10	11	9	5	21
Application & user security (4)	12	15	4	5	27
Automated toolkit use (8)	6	15	9	6	21
Biometrics	2	11	10	11	13
Cloud & multi-tenant cloud security (2)	18	12	6	3	30
Cryptography	9	11	9	8	20
Cyber assurance & compliance (3)	14	15	6	4	29
Cybercrime detection & investigation (3)	13	16	5	4	29
Data loss prevention (4)	12	15	6	5	27
Data visualisation, presentation & graphic design	9	10	7	9	19
Digital forensics	7	11	9	11	18
Disaster recovery & business continuity (6)	9	14	11	5	23
Distributed systems security	7	10	10	8	17
Email & browser security	9	6	11	9	15
Ethical hacking (8)	8	13	7	8	21
Human behaviour, psychology & social eng (5)	6	19	4	7	25
Identity theft	4	14	10	8	18
Information security management (2)	12	18	3	7	30
Legal & regulatory requirements (1)	13	20	3	3	33
Malware & intrusion detection	10	8	10	9	18
Malware packet analysis	7	8	10	11	15
Mobile security (7)	12	10	7	8	22
Network security (6)	9	14	5	9	23
Open source vs commercial tools	8	10	9	8	18
Operating systems	7	5	10	11	12
OWASP Top 10 & SANS 25 (9)	10	10	9	7	20
Penetration testing (6)	9	14	9	5	23
Risk management incl IoT (4)	6	21	4	8	27
Scripting & data processing	6	11	9	9	17
Secure coding, programming, & testing (7)	11	11	6	9	22
Security auditing and certification (6)	8	15	7	6	23
Security intelligence (6)	10	13	7	7	23
Software patterns	3	10	9	12	13
Threat modelling	5	15	8	7	20

Considering the Definites + Probables > 20, the top training needs emerge as:

1. Legal and regulatory (33)
2. Information security management, *joint second* with Cloud & multi-tenant cloud security (30)
3. Cyber assurance & compliance, *joint third* with Cybercrime detection& investigation (29)

Question 3: Certified Professional Scheme. Respondents were asked "*Are you interested in a Certified Professional scheme for cyber security professionals?"*

32 (76%) of the 42 respondents indicated Yes.

Question 4: Involvement in external Collaboration. The next series of questions concerned collaboration practices within the sector. Respondents were first asked "*Has your organization been involved in external collaborations in any area?"*

Table 5: Has your organization been involved in external collaborations in any area? (n=40)	
Areas of collaboration	**%**
R&D	62.5%
Business to Business Collaboration	42.5%
Training	40.0%
Marketing	35.0%
Other areas (please specify).	15.0%

The 'other' areas specified were:

- Mutual collaboration with local CIT college, including a scholarship for one student /year
- Innovation grants via EI
- Bug Bounty Programs or Crowd sourced application testing

Question 5: Types of Collaboration Partners. Respondents were asked "*With what types of organizations have you collaborated ?*". The results show a wide range of collaborations with industry and academic partners.

Table 6: Types of Collaboration partners (n = 40)	
Answer Options	**%**
Irish company/ies	65.9%
Overseas company/ies	73.2%
Overseas parent or legally affiliated company	24.4%
Irish University or IT college	58.5%
Overseas University or college	36.6%
Other organization (please specify)	12.2%

The 'other' organisations specified were:

- Overseas Governments
- Enterprise Ireland
- User Groups ; Peer Groups (HTG)
- Law enforcement agencies and government

Question 6: Interest in future collaboration opportunities. Respondents were asked *"Would you be interested in finding out more about collaboration opportunities?"* and a range of potential areas of collaboration were offered. The responses show a significant interest in collaboration for R&D, and for Business-to-business collaboration.

Table 7: Areas of interest for collaboration (n = 38)	
Answer Options	**%**
R&D	63.2%
Marketing	42.1%
Business to Business Collaboration	60.5%
Training	44.7%
Other (please specify)	2.6%

The only 'other' area of interest specified was in 'algorithmic research'

Question 7: Display of Logo on ISI website. Respondents were asked *"Would you like your company's logo to be included on the ISI website in the membership section?"*

73% of 41 respondents expressed interest, 20% were not interested and 7% needed to check with other company staff, or would require prior approval.

Question 8: What must Ireland do to be recognised as a Centre of Excellence? Respondents were asked *"In your view, what does Ireland need to do to be recognised as a centre of excellence in cybersecurity?"* Free text responses were sought and 34 were received. These are summarised below, with the full list of responses in Appendix 1:

With the goal of Ireland becoming a Centre of Excellence in cybersecurity, the availability of strong talent is the main concern of the companies. As well as a good supply of graduates from third level, the concept of apprenticeships was suggested where they could learn from experienced professionals. The importance of sufficient high quality Third level qualifications in cybersecurity at both under-grad and post-grad levels was highlighted, along with the need for a Research Centre to underpin the growth of the industry here.

Awareness is cited by many companies, both from the point of view of supply of talent by priming pupils at second level, and in terms of awareness of the business community to the risks of cyber breaches and solutions available. In the latter case, it was proposed that there could be 'security tokens' available through agencies such as IDA, EI and LEOs which can be redeemed in a similar way to the 'On-line vouchers'.

The need for a cohesive strategy towards the Centre of Excellence goal was proposed with input and direction from Education, Industry and Government. The survey showed that Ireland has a strong message to communicate internationally in terms of research underway here, multi-national leaders in the sector, Irish SMEs and a host of start-ups. There is significant goodwill evident among the companies to contribute towards the goal.

Question 9: Job creation expectations. Respondents were asked "*How many jobs do you expect to create within your company in the period 2017/2018?"*

Table 8: Expected no. of Jobs in 2017/18 (n = 41)	
No. Jobs to be created	**%**
0-5	40.5%
6-10	19.0%
11 or more	40.5%

This produced a strongly positive response, with 40% of companies expecting an extra 0-5 jobs, and a further 40% anticipating 11 or more, with the remainder anticipating 6-10 jobs.

Question 10: What else can ISI do for members. Respondents were asked "*What else would you like InfoSecurity Ireland to do for you and your company?.* This was also a free text answer which received 23 responses. The full list of responses is in Appendix 2, with the major recurrent suggestions being:

- Networking & information activities promoting awareness, collaboration, community building, thought leadership, feedback.
- Policy development/lobbying
- Overseas Promotion via RSA type events and connection with overseas experts.

Appendix 1: What must Ireland do to be recognised as a Centre of Excellence in cybersecurity

- *Better talent, more focus on cybersecurity at 3rd level,*
- *I think awareness is the key and it starts at the point of entry to technology. Gamify cybersecurity awareness programmes to drive awareness. Back this with a national quarterly "online" event (try to set a Guinness world record for attendees, with 2 key speakers on a cyber topic one that speaks to the problem one that speaks to the solution. Make it a global event and brand it. Follow the early adaptors (primary and secondary school awareness) with relevant dynamic third level programmes. Extend the awareness programme to everybody and make it fun.*
- *Many new job descriptions are now cited as Cyber Security Specialists. Also customers are really concerned about the unknown and high risk factor associated with Social Engineering and Ransomware*
- *Ireland must invest in training on cybersecurity at all levels of the education ecosystem. It must also make deliberate efforts to ensure that there is close collaboration between educational and research firms with security companies.*
- *Develop a cohesive strategy to suit its particular market with input and direction from Education, SME, Business leaders and Government. Possibly similar to the UK Cyber Essentials scheme but tailored for Irelands specific needs (i.e. the majority of businesses are micro). There should also be an extensive education and training programme for Cyber and Information Security which should cover all of the areas identified and listed in the training needs above. Industry professionals and specialists could be utilised to provide depth and experience. Ireland needs to recognise that in the world of information and cyber security it is no longer an island in the Atlantic but a key player in the world stage hosting some of the worlds largest brands. Another idea would be to roll out an apprenticeship type programme thereby engaging those who are interested and learn from experienced professionals.*
- *A National Research Centre in cyber-security that brings together all the expertise in Ireland.*
- *Build on the Technology base that we already have*
- *Provide a pool of trained and Qualified Cybersecurity Professionals*
- *Embrace innovation*
- *More research / 3rd level courses*
- *Keep highlighting it*
- *Develop strong skills base as you advocate, support innovation and startups in balance with MNC incentives to foreign firms*
- *As well as participating in more research we need to publicise the research that happens on the island.*
- *We need to continue to build on what we have started here. This includes InfoSec Irish startups (Barricade for eg), FDI, educational courses at MSc Level and meetup groups such as CorkSec. We are lacking in experienced senior level Security Engineers, we need to ensure we are developing people to senior levels to be able to staff high level positions as they become available here. We should have more certified engineers here, EG < 400 CISSP, compare that to CCNA/CCNP/CCIE for eg. There are also areas for us to improve on in promoting Ireland's existing achievements in the InfoSec domain abroad through agencies such as the IDA. There are some conferences here but nothing on a world scale such as InfoSec Europe or RSA. The WebSummit did a lot for publicising the startup community here, perhaps attracting a major conference or starting our own (Ack that we have some already) would help. EG, IT@Cork conference 2016 was very successful and included a section on InfoSec, we should leverage this organization more and do something security related with them.*
- *Hosting International seminars/workshops/conferences on cyber security. Dedicated academic/industrial research hub. More government investment in attracting Cyber Security R&D.*

More Investment in ICT infrastructure. Dedicated Cyber Security Post-Grad courses (including transition courses from other disciplines)

- *Policy direction and public commitment from Irish government to protect Irish cyberspace. Without this leadership other efforts will struggle to succeed*
- *I think the assertion that it can be a global leader in InfoSec at the deep product level is not viable, as countries which lead in this space have developed defence industries with large scale govt investment - simply not achievable in Ireland. However, Ireland can lead in respect to the application of best practice to data centers and information resources. Though in reality this means having a deep talent pool - and credible certification can help this. We have a disproportionately large footprint of US West Coast Tech companies which help develop the domestic talent pool - and this creates a sizeable competence in addition to what can be produced by domestic organisations and colleges. We can play much larger than our size and some recent FDI investments underline this.*
- *Have a number of core Security & Privacy and Cryptography courses at the Masters level to produce a constant stream of high trained professionals who will then feed into the relevant industries*
- *Not sure, but i think this objective is a long way off, other than a few individuals, I don't feel there is currently any international recognition of Ireland as any kind of centre of cyber security.*
- *Ongoing outreach and promotion of the country as uniquely positioned to operate in this space from a technology and EU perspective (especially in context of Brexit)*
- *Deliver free/low cost training. Get actual government buy-in such as security assessment "tokens/coupons" for SME's in order to make businesses more secure.*
- *An agency with funding to deal with this at a national level, that agency to have responsibility for security, their advice recommendations to be taken seriously.*
- *Develop a comprehensive cybersecurity R&D funding strategy at a national level.*
- *A structured approach to centres of excellence within agreed locations.*
- *Establishing SFI centre would help*
- *Market Ireland, and keep the skills within Ireland*
- *Thought leaders, R&D.*
- *Establish forums that are active and recognised in pushing forward Ireland's position as a leader in InfoSec - we already have it in data protection, why not in InfoSec? We could have a government standard for all public sector organisations and private sector companies.*
- *A business culture that promotes security, moving it from only IT / audit / legal spheres*
- *Create higher skilled engineers as opposed to security managers. Managing security at the business level to me is of course a positive step in the right direction but without engineering expertise at a server/application level it's fairly worthless. Malicious actors don't care how your company is managed, they attack what's exposed at a technical level.*
- *Engage with experts outside of Ireland - we can help*
- *We need to make security products accessible to SMEs.*

Appendix 2: What else can ISI do for members?

- *Keep networking and grow the ISI membership*
- *Arrange more workshops to provide a space for collaboration and networking*
- *We are interested in all aspects of Information and Cyber Security and would welcome the opportunity to widen our contacts and share experiences.*
- *Facilitate collaborations*
- *Peer to peer marketing and research groups.*
- *We have had challenges in recruiting senior Analysts and team leads, any assistance with advertising open positions would be useful. Fostering a community between Security operations*

centres (SOC) would also be very interesting to us. We have begun a relationship with another SOC recently and visited their operation which was extremely interesting.

- *Establish influential working groups to develop policy recommendations for government. Providing networking opportunities for members. Developing cross-sectoral relationships and partnerships*
- *Networking opportunities Events*
- *Promoting and presenting thought leadership pieces is of value. Note our business in Ireland is focussed on Financial Crime, the Infosec business is largely resourced out of the UK.*
- *Networking events. Possible joint marketing engagement*
- *Help promote Irish Cyber companies. Open a direct line to the government so they can sponsor companies to attend events such as RSA, Infosecurity Europe - E.g. France, Israel, Northern Ireland, Germany and Spain all had stands promoting their regions companies at InfoSec.....*
- *Raise awareness around Authentication solutions such as FIDO as the world continues to move towards mobile where traditional factors (smart cards, tokens etc.) become redundant.*
- *Collaboration opportunities with new and existing Irish & Global corporates in this area.*
- *I'd like to see more events*
- *Maybe a monthly or quarterly newsletter updating members on what others members are up to, possible collaborations, external events, etc.*
- *Education & awareness of end users/companies to the risks through open days / seminars*
- *Promote infosec at 'C' level across Ireland*
- *Provide more statistics of the current security landscape or threat information.*
- *We could help connect Infosecurity Ireland with security experts in New York*
- *Provide feedback on security concerns from other members, so that we can consider alleviating those via our new product features.*

InfoSecurity Ireland

InfoSecurity Ireland (ISI) is an association of information security software companies with a membership of some 130 companies and colleges. Its objective is to present Ireland as a centre of excellence in cybersecurity, with consequent benefit for revenues and jobs in those companies.

ISI works to connect the players in the infosecurity community to share their knowledge and best practice so that the combined resource operates as a dynamic ecosystem.
ISI is supported by the development agencies of IDA and Enterprise Ireland.

Further information on ISI is at www.infosecurityireland.org

Enquiries relating to this survey should be addressed to Jim Cuddy, Coordinator InfoSecurity Ireland at jim.cuddy@gmail.com

10th October 2016