

Client: Skillnets Limited
Source: Techpro
Date: 01/09/2018
Page: 13
Reach: 7000
Value: 3494.16

Cybersecurity Skills Conference

Filling the Cybersecurity Skills Gap

AS the cybersecurity threat increases Ireland continues to have the highest demand of any country worldwide for cybersecurity jobs, while at the same time reporting a worrying talent shortage now and in future years with an increase of over 40% in Cybersecurity vacancies in the space of 2 years.

Further and better training and more entrants to high level cybersecurity programmes will help to reduce this shortfall but it is now obvious that to make any dent in the skills gap we need to attract more young people, women and non-computing graduates into cybersecurity roles.

And any drive for new talent must be accompanied by an equal focus on broadening the base of cybersecurity skills across all functional areas as well as working hard to retain existing cybersecurity staff.

This event will see the launch of a new Cybersecurity Skills

Initiative (CSI) aimed at tackling this problem which brings together a broad coalition of industry, academic and government partners to be led by Skillnet Ireland.

Conference Workshops

Cybersecurity Primer for CEOs – What to know so you know what to do

COMPANIES are either too confident or underprepared to deal with security breaches and cyber attacks – and these can cause enormous damage. One third of Irish and Northern Irish businesses suffered a data security breach last year, causing damage to their businesses.

An overwhelming majority (93%) of companies believe the complexity of threats they will face over the next 12 months will increase and nearly half (46%) admit they will either struggle to deal with this or that threat defence will be impossible.

Irish companies mirror the global picture reporting a surge in requirements for enhanced cybersecurity due to increased regulation on data privacy (GDPR) cited by 73% of respondents to a Deloitte study, more sophisticated scamming and phishing (59%), and growth in identify



Client: Skillnets Limited
Source: Techpro
Date: 01/09/2018
Page: 13
Reach: 7000
Value: 3494.16

theft (53%).

This workshop will explore -

- Why cybersecurity is a business issue not just an IT issue
- Necessity of investing in security awareness training
- What cybersecurity technologies to deploy
- Cost-benefit analysis of investing in cybersecurity prevention measures
- Outsource or build in-house capability
- Encouraging vulnerability reporting by staff at every level
- How to manage recovery after an attack and adapt future processes
- Risk of being too slow to detect and respond

Target Group: C-level executives, managers, and owners and managers of small and medium companies.

Any sector - any size



Risk Assessment for companies

UNDERSTAND, list, assess, grade and plan how to fix cybersecurity vulnerabilities

Most computer

defences are so weak and poorly managed that they can be relatively easily breached. But if individuals and organisations took some simple steps, they could quickly and dramatically reduce the impact of cyber crime. The problem for most companies is the absence of real accurate and meaningful data to make good decisions. Because of this some organisations may be applying resources in the wrong places to defend against the wrong threats. Without an analysis of how well the organisation is geared to defend against breaches we cannot implement remedial actions or make good management and investment decisions.

This workshop will explore these issues and use a structured tool to enable participants make an initial assessment of their cybersecurity preparedness. This is a tailored example that gives a flavour of what is involved in risk assessment. It will examine areas as complex as cloud security and business continuity management after a breach, down to issues like Passwords, Patching; Phishing, Protecting against Ransomware and Malware, Device Configuration, Backups and having an effective Business Continuity Plan.

The aim is to help participants identify any weakness in your defensive strategy and operational procedures and maximise the chances of effective recovery from a disaster.

Target group: C-level executives, managers, owner-managers, practitioners and technical staff with ICT responsibilities. Any sector - Any Size.



Become a Cyber Hacker for a Day!

TEAMS of 4 'greenhorns' (non-cybersecurity specialists) from different companies competing to defend against cyber attacks in real time.

This session running continuously over three hours (with unlimited coffee!) in the main Conference Hall will introduce complete beginners to cyber hacking. They will learn how to hack a website, break into servers and steal computer files. Capture the Flag is a fun and safe environment to learn what hackers do and the tools they use. It will also demonstrate how vulnerable computer technology is and help participants to become more aware and skilled at securing and defending against attacks.

Participants will be formed into teams of 4 which are posed a series of problems that increase in difficulty. Teams attempt to earn the most points, but do not directly attack each other. Rather than a race, this style of game play encourages taking time to approach challenges and prioritise the quantity of correct submissions.


Target Group: The workshop is aimed at non-security technicians. A company may send their own team of 4 participants. If you have less than four then your participant(s) will be teamed up with participants from other companies. No cybersecurity skills are required - In fact we really do want 'greenhorns' with no prior cybersecurity skill, so anyone with basic computing knowledge (how to surf and search, etc) and who enjoys solving puzzles will be welcome. All that is required is to bring your own laptop. You must pre-register and you will then be given some online examples to look at before you come. The top 3 teams will be awarded prizes. ■



Client: Skillnets Limited
Source: Techpro
Date: 01/09/2018
Page: 13
Reach: 7000
Value: 3494.16

Topics Covered:
AS WELL AS OUTLINING THE NEW INITIATIVE THE EVENT WILL HEAR FROM A RANGE OF EXPERTS:

- **Where's the Risk? Examining the Threat Landscape**
Brian Honan, CEO, Irish Reporting & Information Security Service
- **Challenges for Higher Education in delivering on the cybersecurity skills agenda**
Dr Anthony Keane, Head of School Informatics and Computing, IT Blanchardstown
- **Criminals Follow the Opportunities - Big or Small**
Detective Supt Michael P Gubbins, Head of the Garda National Cyber Crime Bureau
- **Using the Power of e-learning**
Speaker from Pluralsight
- **Build from the Inside Out**
James B Alvilhiera, World Wide Sales Leader & Cyber Security Expert, IBM Watson Talent
- **AI is the future of Cybersecurity for better or worse!**
Panel Discussion led by Paul Hearn, Editor of Tech Pro



For more information and to register visit: ictskillnet.ie