TAPPING INTO CYBER SECURITY TRAINING

The alarming rise in the number of data breaches and ransomware attacks now signals the need for every organisation to take measures to prevent or minimise the impact on their business, according to Jan Carroll, UCD lecturer and cyber security researcher. And with a global shortage of cyber security professionals, she outlines a selection of training courses for those who may wish to upskill or reskill in this sector.

Ransomware attacks are on the rise and are set to cost organisations $6 trillion globally in damages in 2021.

Modern ransomware, such as the one which impacted the HSE in May, uses a 'two-pronged attack' that takes down systems and holds client data to ransom, thereby threatening a data breach.

This type of malicious software is designed to block access to systems and files until a ransom is paid. Managers need to get into the mindset of preparing for 'when' and not 'if' they are hit by ransomware. Every organisation, regardless of size, can and must take measures to prevent or minimise the impact of a ransomware attack.

These measures included the following:

- Identify critical data and systems and prioritise for back-up
- Create and test back-ups regularly
- Create a Cyber Incident Response Plan
- Establish regular patching and updates
- Educate and support staff in regular cyber awareness training
- Employ email filtering
- Use an intrusion detection system
- Use whitelist applications

The National Cyber Security Centre (**www.ncsc.gov.ie**/) offers advice on how businesses can improve their security defences over a 12-month period. For details check out '12 Steps to Cybersecurity for Irish Businesses' on the NCSC website.

RESPONDING TO RANSOMWARE

So, what happens if you're hit with a ransomware attack? Firstly, the criminal attackers will let you know, often with a pop-up declaring the attack and the terms of the ransom.

Surprisingly, the larger organised crime gangs are essentially run like well-funded corporations. This includes 'customer' support teams who help the victims through the process if they decide to pay the ransom and recovery of their systems and data.

The seven steps to take…

1. Remove the device from the network.
2. Implement a Cyber Incident Response Plan.
3. Establish the source and scope of the attack.
4. Notify the National Cyber Security Centre and An Garda Síochána.
5. Do not pay the ransom.
6. Access the 'No More Ransom' site for advice and tools to recover files from known ransomware attacks from https://www.nomoreransom.org/en/
7. If no other option is available, restore files from recent back-ups.

Modern ransomware, such as the one which impacted the HSE in May, uses a 'two-pronged attack' which takes down systems and holds client data to ransom, threatening a data breach.

UPSKILLING ON CYBER SECURITY

A Cyber Ireland Skills Survey recently reported that nearly half the number of all cyber security roles are currently unfilled. With the colleges churning out plenty of new graduates, it will take years to fill the gaps. This presents the perfect opportunity for those who may want a change of direction in their own careers.

If you're someone who wants to move into the cyber security industry and bring your professional and life experience with you, how do you do it, and what pathways are open to you?

The good news is that there's a plethora of quality, affordable (or free) courses to get you started on your move to an exciting, well-paid, and sought-after role. Here are details of the range of courses and certification levels offered by some mainstream training providers.

Cyber Quest: Cyber Quest is a new initiative from **www.itcorkskillnet.ie** to upskill and reskill those whose employment has been impacted by the pandemic. All training is online and self-paced focusing on cyber skills training. There are three pathways depending on your starting point and all courses are free. They also have a busy jobs board for placing qualified applicants.

Cyber Skills: This collaborative initiative addresses the skills shortages in the cybers security sector, offering a range of fee-paying online courses for those with some technical skills who may wish to upskill or reskill in cyber security.
Details: **www.cyberskills.ie**

Further Education & Training Course Hub: The FETCH Hub courses are available on the national further education and training sector. Search the term 'cyber' for a range of online and class-based courses, including CompTIA Cyber Security Analyst (CySA+).

The Hub also provides access to the national network of Adult Education Guidance supports for help finding the right course for your needs.
Details: **www.fetchcourses.ie/**

Ecollege: Ecollege is the 'best kept secret' in Irish education as it is such a fantastic resource to anyone wishing to upskill, especially now as all courses are free to aid those impacted by the current Covid pandemic.

This online college is backed by SOLAS and the courses are available to those over 18 years and living in Ireland. Details: **www.ecollege.ie**

FIT Associate Apprenticeship – Cyber Security: Facilitated by FIT (Fast Track to Technology), this is an excellent option for individuals wish to 'earn while they learn'.

Suitable applicants receive six months training prior to being placed with an organisation to learn on-the-job while completing their studies. Details: https://fit.ie/course/fit-ict-associate-apprenticeship-cyber-security/

ICT Skillsnet & CISCO: ICT Skillsnet and CISCO offer the CISCO Networking Academy training courses, which are a great place to start for those new to cyber security as their courses are self-paced and include quality video content. Details: www.ictskillnet.ie/training/ict-skillnet-cisco-networking-academy/

ICS Skillsnet & NCI: ICS Skillsnet has partnered with the National College of Ireland (NCI) to offer the Masters of Science in Cyber Security.

This grant-aided course is outstanding value for eligible candidates who work in private or commercial semi-state organisations in Ireland. Intake starts in January 2022 and applications are now open. Details: www.ictskillnet.ie/training/masters-of-science-in-cybersecurity

ICTTF – International Cyber Threat Task Force: Cyber security consultant Paul C. Dwyer and his team have put together a range of excellent professional courses for those working and wanting to progress in the cyber security industry. Some courses are available in conjunction with ICT Skillsnet and the Irish Computer Society. The ICTTF also offers a free Cyber Security Bootcamp for Women and is an excellent foundation for women who want to learn more about cyber security. Applications are now open. Details: https://community.icttf.org/courses

ITAG – Innovation Technology AtlanTec Galway: Innovation Technology AtlanTec Galway (ITAG) offers the Cyber Security Analyst Bootcamp for Jobseekers. Fantastic opportunity to upskill quickly to gain the skills and support to start a fulfilling and well-paid career. Details: https://itag.ie/events/cyber-security-analyst-bootcamp/

Future Learn: The Open University is behind these courses, and offer free courses including the 'Introduction to Cyber Security' which is perfect for complete cyber novices and another good starting point for those wanting a taster or just learn how to secure themselves online. Details: www.futurelearn.com/courses/introduction-to-cyber-security

UCD Professional Academy: The UCD Professional Academy offers a range of short professional courses that covers a wide range of popular topics, including a Professional Diploma in Cyber Security (which I created and deliver myself). A Professional Diploma in Ethical Hacking is also available. Courses are delivered completely online with regular intake. UCD Professional Academy offer an attractive corporate discount, often with 50% off eligible group bookings. Details: www.ucd.ie/professionalacademy/

For courses run by Irish colleges and universities check out Cyber Ireland's course finder at https://cyberireland.ie/course-finder/. There's nothing stopping you to take the first step to gain an exciting and specialised career which can take you anywhere in the world.

ARMED AGAINST PHISHING

The most popular attack vector for ransomware to enter your network is via an email phishing attack where an employee is tricked into clicking on a link in an email. There are technical controls to prevent many of these emails, however, these emails have become much more targeted and sophisticated, using well-honed social engineering techniques.

Anyone is susceptible to clicking on these links, even the most cyber aware individuals. By instilling a security culture from the top down with embedded awareness training and support, your organisation will be much safer and secure, and your team will improve their security practices across all areas of their lives.

It is also vital that there is an 'no blame' culture, so that employees are free to report incidents and will be supported, not reprimanded if their actions provide access to an attack.

An example of the 'Recovery Service' pop-up from the CONTI Group who attacked the HSE in May 2021. https://sensorstechforum.com/ittzn-virus-file-remove/

Recommended resources to improve cyber awareness:

* **Cyber Readiness Institute** offers free, online, structured training, and all team members should take a Cyber Readiness Programme, which focuses on four awareness areas – Passwords, Software Updates, Phishing/USBs, and Removable Media. Details: https://cyberreadinessinstitute.org/

*** Cyber Leader Programme** is recommended for your organisation's cyber champion; this person does not need to hold a technical role, but just be passionate about improving the team's cyber awareness. This course is more involved but includes essential elements such as identifying critical assets and creating the Cyber Incident Response Plan.

*** Cyber Awareness Interdisciplinary Consortium Ireland** enables infographics and awareness videos to be shared with your network. An interactive tool from Google is also included to 'Test your ability to spot phishing emails', so everyone should have a go. You will learn how to spot the fakes. Detail:s: www.caici.eu/test-your-ability-to-spot-phishing

Everyone in an organisation needs to know that security is taken seriously and nobody is exempt – from the managing director, the delivery person to all clients who walk through the door. Security policies, procedure and practices must be consistently implemented to maintain your security posture. A secure culture keeps everyone safe and it's good for business.

Reference:
https://gomindsight.com/insights/blog/protect-your-business-rise-in-ransomware/

ABOUT THE AUTHOR

Jan Carroll, UCD Professional Academy lecturer and cybersecurity researcher, has a passion for teaching and learning and is working to close the cyber skills gap by encouraging more women and underrepresented groups into the cybersecurity industry.

Jan holds a MEd and MSc in Cyber Security, and currently works with SMEs to rebuild and secure their businesses following the impact of Covid-19. She mentors women who, like herself got into infosec (information security sector) after the age of 40.