The following excerpts are sourced from two online articles that examine the current impact of technology in protecting Irish businesses against cyber attacks, along with data from the National Cyber Security Annual Update 2023. Detailed references for all the content are provided below.

In this week's news feature, MSN.com (2024) talks to head of Dell Ireland on the key cyber threats for Irish business and the role of people and technology in protecting an organisation from cyber attack. In related news, RTE (2024) published data from the National Cyber Security Annual Update 2023 in response to public demand for greater transparency of cyber events and the announcement of increased grant aid for SMEs.

Dell chief says skills training vital in using AI to counter cyber risks.

In an interview with the MD of Dell Ireland, MSN.com (2024) explores how Irish organisations can benefit from enhancing their cybersecurity efforts and demonstrates how artificial intelligence is now at the heart of both cybersecurity and cybercrime. In summary, GenAI has emerged as a double-edged sword in defending businesses against cyberattacks.

> Jason Ward, EMEA North vice-president and managing director of Dell Technologies Ireland, says that cybersecurity isn't just about technology; it's fundamentally about the people who use and safeguard it. In this Q&A interview, Mr Ward outlines how Irish organisations can benefit from enhancing their cybersecurity efforts. Cyber Ireland estimates that 10,000 additional jobs could be created within the cybersecurity sector by the end of the decade, offering a significant opportunity for Ireland to take the lead in this critical area. Artificial intelligence (AI) is no longer a distant concept — it's here, reshaping Ireland's business landscape at an unprecedented pace. From healthcare to finance, transportation to manufacturing, Generative AI (GenAI) is solving complex challenges and informing better decision-making. The shift towards accelerated computing is also revolutionising productivity levels, much like the industrial revolution, with potential gains of 20-40%.
>
> According to the Dell Technologies Generative AI Pulse Survey, 76% of IT leaders believe that GenAI will have a significant, if not transformative, impact on their organisations. But, as GenAI continues to evolve and develop, so does its impact — for both cybersecurity and cybercrime. GenAI has emerged as a double-edged sword in the cybersecurity landscape. It holds immense promise as a powerful tool to enhance data protection and threat detection, yet it also opens new avenues for cybercriminals.
>
> MSN.com (2024)

Over recent months, we have seen several high-profile cyber incidents both here in Ireland and globally that reinforce the need for organisations in both the public and private sectors to enhance their cyber resilience in our AI era.

SMEs are particularly vulnerable to attack. According to the Garda National Cyber Crime Bureau, the number of ransomware attacks targeted at SMEs continued to grow last year. Infected emails and email links, fraudulent websites, and fake invoice payment requests from suppliers are some of the ways in which SMEs are being targeted. With the growing volume of data which need to be kept secured, many SMEs feel overwhelmed.

The Cyber Security Review Grant unveiled by Enterprise Ireland and the National Cyber Security Centre (NCSC) last month is a positive first step in enhancing the cyber resilience of the Irish business community.

MSN.com (2024)

Dell Technologies Ireland sees a rise in companies strengthening their AI cyber resilience. It believes that every organisation must understand cyber threats and place greater emphasis on the role of AI. According to MSN.com (2024), the reliance on traditional firewalls and antivirus software is becoming outdated, and employees will increasingly contribute to cybersecurity efforts.

We're seeing businesses increasingly turn to advanced technology to double down on their resilience, says Mr. Ward of Dell Ireland. GenAI is increasingly being used to detect threats faster, predict potential cyber-attacks and automate security processes. Our latest Innovation Catalysts Study revealed that 3 in 4 organisations in Ireland now use automated tools to detect and respond to cyber threats. This powerful technology is also helping organisations to adopt a Zero Trust model. Instead of assuming that anyone working inside your network is trustworthy, this model ensures that access to data and systems is continually verified and detecting unusual behaviour. When AI identifies suspicious activity, it can initiate recovery protocols automatically, such as securing critical data in a Cyber Recovery Vault—a highly secure and isolated repository for critical information. This level of automation significantly reduces downtime, allowing businesses to recover more quickly from cyberattacks and resume normal operations with minimal disruption.

Cybersecurity isn't just about technology; it's fundamentally about the people who use and safeguard it. While AI and advances system provide defence against cyber threats, they are only as effective as the individuals who implement, manage, and interact with them. Human error remains one of the leading causes of data breaches, making it essential to empower employees to be the first line of defence. This is where robust cybersecurity training comes into play. It can help change user behaviour by fostering a culture of vigilance and responsibility. By educating employees on best practices and the threats they are likely to face during their working day, organisations can significantly reduce the likelihood of breaches.

MSN.com(2024)

AI can also play a helping hand. The technology can be used to tailor and personalise cybersecurity training programmes depending on an employee's role, access level, and previous interactions. This ensures that high-risk users receive the training that they need, when they need it.

MSN.com(2024)

As we mark the end of Cybersecurity Awareness Month, it is vital that leaders in every organisation understand the cyber threats they face and place a greater emphasis on building cyber resilience in the AI era. Cyber Ireland estimates that 10,000 additional jobs could be created within the cybersecurity sector by the end of the decade, offering a significant opportunity for Ireland to take the lead in this critical area. By enhancing their cyber resilience, Irish firms can not only safeguard their operations but also position the country as a global leader in cybersecurity, particularly as AI becomes more integrated across industries. The Government's National AI Strategy points out that a strong approach to security is key to maximising trust in AI and a key ingredient to strengthening Ireland's position as a global leader in AI-driven innovation. Furthermore, as businesses face new obligations under the EU's Network and Information Security Directive, the need to prioritise cyber defences has never been more urgent. At Dell Technologies Ireland, our team of experts are building the next generation cybersecurity solutions and essential infrastructure for organisations to protect their most important information assets. But, as cyber threats become more sophisticated and costly, employees must be empowered to become the front line of their cyber defence.

By continually fostering a culture of cyber resilience that leverages the power of AI and other emerging technologies while equipping people with the necessary cybersecurity skills, businesses—small, medium, and large—can stay ahead of evolving cyber threats.

MSN.com (2024)

Over 700 cybersecurity incidents in Ireland last year

As Black Friday is fast approaching, the timely release of the National Cyber Security Annual Update 2023 (Ireland), as reported by RTE (2024), underscores that most incidents in the region were classified as low in severity. Much of the credit for this success goes to the National Cyber Security Centre and its proactive efforts behind the scenes:

> The National Cyber Security Centre (NCSC) received 5,276 reports last year, 721 of which were confirmed as cybersecurity incidents. This led to the opening of 309 investigations. The figures are contained in the National Cyber Security Annual Update 2023 which was published today. According to the report, the vast majority of incidents were categorised as being at the lower end of the severity scale. There were no incidents reported that were deemed severe enough to be in the top two categories. This shows the successful preventative work being done by the NCSC to ensure threats are being stopped before they can severely impact the State's infrastructure," the report states.
>
> The annual update is being released to mark the mid-term point of the National Cyber Security Strategy and details the work done by Government departments and agencies in the fight against cyberattacks. The report contains inputs from the Department of Communications, the NCSC, An Garda Síochána, the Defence Forces, and the Department of Foreign Affairs.
>
> "This update comes as a direct response to the public's calls for more frequent reporting, for greater insight, and transparency into the Government's efforts in the cybersecurity arena," said Minister of State at the Department of the Environment, Climate and Communications Ossian Smyth.
>
> "What this annual update shows is that the Irish government is committed to protecting the State's critical infrastructure, developing skills and capacity in civil society, and safeguarding Ireland's continued digital transition," Mr. Smyth said. The Government has also announced the launch of a €2m fund to provide grants to small and medium enterprises (SMEs) as they enhance their cybersecurity. The new initiative is co-funded by the European Union's Digital Europe Programme and will offer companies financial support to strengthen their IT systems. Eligible SMEs can apply for funding of 80% of project costs, with a maximum grant of €60,000, to implement key cybersecurity measures, re-test their systems, and receive expert guidance for future improvements.
>
> RTE (2024)

References:

MSN.com (2024). 'Dell chief says skills training vital in using AI to counter cyber risks'. MSN.com, November 4th .Available at: https://www.msn.com/en-ie/money/companies/dell-chief-says-skills-training-vital-in-using-ai-to-counter-cyber-risks/ar-AA1tjNFY?ocid=BingNewsVerp
(Accessed 13 November 2024).

RTE (2024). ' Over 700 cybersecurity incidents in Ireland last year'. RTE (2024) November 5th. Available at: https://www.rte.ie/news/business/2024/1105/1479075-cyber-security-reports/. (Accessed 08 November 2024).

EON- 21-11-24

SEASPRAY PRIVATE
Creating Investment Solutions