Cyber Resilience Survey 2022

DELL Technologies in partnership with THE EXECUTIVE INSTITUTE & sponsored by intel

FOREWORD

Securing Digital Transformation

Jason Ward
Vice President & Managing Director,
Dell Technologies Ireland

As we look back over the last two years, it's clear there has been a seismic shift in how business leaders perceive technology and its role in shaping a do-anything-from-anywhere economy.

This trend is only set to continue and accelerate. Leaders have witnessed the power of technology to make their business more agile, efficient and innovative and there is no turning back. Today, its estimated that 65% of global GDP this year will be digital.

However, as the pace of digital transformation accelerates, so too is there a growing need for businesses to place cyber resilience at the heart of their digital transformation journey. After all, success in a digital economy relies on the ability of businesses to secure data and maintain trust in their IT systems.

With cyberattacks occurring globally every 11 seconds, for businesses around the country it's no longer a matter of "if", but "when". In order to truly thrive in the digital era, it's crucial that leaders focus not only on the power of new technologies to transform their business, but also on importance of putting measures in place to mitigate against, respond to and recover from the growing threat of cyberattacks

In order to better understand the cyber resilience landscape for Irish businesses, Dell Technologies has partnered with the Executive Institute to gain an insight into business leaders' changing attitudes towards cybersecurity, as well as the steps taken by Irish businesses to enhance their cyber resilience in a data-driven era.

The Cyber Resilience Survey 2022, which gathered responses from senior leaders in a diverse range of sectors, shows that while businesses are focused on strengthening the cyber resiliency of their organisation, many are struggling to put in place the tools and expertise needed to withstand and recover from a cyberattack.

> *With cyberattacks occuring globally every 11 seconds...it's no longer a matter of "if", but "when".*

While 91% of organisations in Ireland recognise the importance of cyber resilience at the senior leadership level, over half of those surveyed identified the ever-growing number of cyber-attacks as the main barrier to enhancing their cyber resilience, followed by outdated technology, insufficient in-house cyber skills and upfront investment.

In addition, although Irish businesses are awavre of the negative business impacts of a cyber-attack, less than a third say they have a well-defined incident response strategy in response to an attack.

These findings point to a growing need for business leaders across Ireland to ensure that the importance assigned to cyber resilience within their organisations is reflected in the strategies, infrastructure and resources they have in place to withstand and recover from a cyberattack.

At Dell Technologies, our team of cyber experts have been helping business leaders across the country to tackle these challenges head on and build a resilient infrastructure where business critical data can be protected amidst a landscape of ever-evolving cyber threats.

By prioritising cyber resilience today, business leaders across Ireland can be better prepared, not just to survive a cyber-attack, but to ensure the success of their own digital transformation plans, safely unlocking the power of technology in a data-driven age.

Jason Ward, Vice President & Managing Director, Dell Technologies Ireland

> *businesses are focused on strengthening the cyber resiliency of their organisation*

CYBER RESILIENCE SURVEY

Introduction

With the onset of the COVID-19 pandemic in Ireland two years ago, many businesses, large and small, embraced technology at an unprecedented speed. From enabling much of the population to work from home to transforming business models, technology is now at the very heart of a truly digital economy and society.

This acceleration in digital transformation is leading to firms generating, demanding and collecting more data than ever before. But this does not come without its challenges. The move to embrace greater digitisation in all sectors of the economy has increased opportunities for cyber criminals and other actors to launch attacks which undermine Irish businesses.

Amidst the growing link between digital and cyber resilience, Dell Technologies has partnered with the Executive Institute, Ireland's premier network for senior leaders, to undertake the 2022 Cyber Resilience Survey. 113 business leaders across a wide range of sectors participated in the survey which was conducted in April this year.

Survey Findings

The latest 'Cyber Resilience Survey' undertaken by the Executive Institute on behalf of Dell seeks to understand business leaders' changing attitudes towards cybersecurity and the steps taken by Irish businesses to enhance their cyber resilience in a data-driven era.

1 CYBER RESILIENCE IS A SENIOR LEADERSHIP PRIORITY

The survey has found that cyber resilience is now a priority for business leaders in Ireland, with 91% of organisations recognising its importance at the senior leadership level.

This comes amidst high profile cyber-attacks witnessed in a range of sectors in Ireland over the past year. These attacks have showcased the ever-changing nature of cyber risks facing businesses.

91%

recognise the importance of cyber resilience at a senior leadership level

2 BUT SEVERAL CHALLENGES REMAIN TO STRENGTHENING CYBER RESILIENCY

55% of those surveyed identified the ever-growing number of cyberattacks as the main barrier to enhancing their cyber resilience followed by outdated technology (20%), insufficient in-house cyber skills (16%) and upfront investment (12%).

55%

pinpoint the ever-growing number of cyber attacks as the main barrier to enhancing cyber resilience

3 HYBRID WORKING TO INCREASE LIKELIHOOD OF A CYBER ATTACK

69% of businesses believe hybrid working arrangements will increase the chances of a cyber-attack or incident. Amid the evolving world of work, a vast majority of businesses surveyed (91%) took steps to enhance data protection in the past 12 months.

69%

of business leaders believe hybrid working will increase the likelihood of a cyber-attack

MANY BUSINESSES LACK DEDICATED CYBER RESPONSE STRATEGY

Although Irish businesses are aware of the negative business impacts of a cyber-attack, only 28% say they have a well-defined incident response strategy in response to an attack.

Moreover, less than a third have stated they would restore the data lost from a standard back-up solution.

28%

have a well-defined cyber attack response strategy

KNOWLEDGE GAP HAS EMERGED AMONGST BUSINESS LEADERS

Despite the growing attention placed on cybersecurity by business leaders, the Cyber Resilience Survey reveals a knowledge gap in the data protection options open to Irish businesses. Close to 6 in 10 business leaders don't know how their business would react in the event of a ransomware attack.

64% of business leaders say they are not sure their organisations have the capability to isolate or "air gap" critical data in the event of ransomware attack.

91%

have taken steps to enhance data protection in the past 12 months

GROWING BELIEF THAT CYBER RESILIENCE IS KEY TO DIGITAL TRANSFORMATION

Looking to the future, 92% agree that enhancing their organisation's cyber resilience is important to ensuring the success of their digital transformation plans.

Business leaders increasingly understand that their organisation's ability to embrace AI, Cloud, Edge Computing and 5G at speed requires is now firmly linked to its ability to protect applications, infrastructure and data in unison.

92%

of leaders agree that enhancing cyber resilience is vital to the success of their digital transformation plans

STRENGTHENING CYBER RESILIENCE IN A DATA-DRIVEN ERA

Protecting Your Most Valuable Asset

In light of the findings of the survey from Dell Technologies and the Executive Institute, how can Irish organisations best protect their most valuable asset – their data?

At Dell we have been supporting Irish businesses with the expert advice and tools to strengthen their cyber resilience. In essence, cyber resilience is an organisation's ability to prevent, respond to and recover from cyber-attacks.

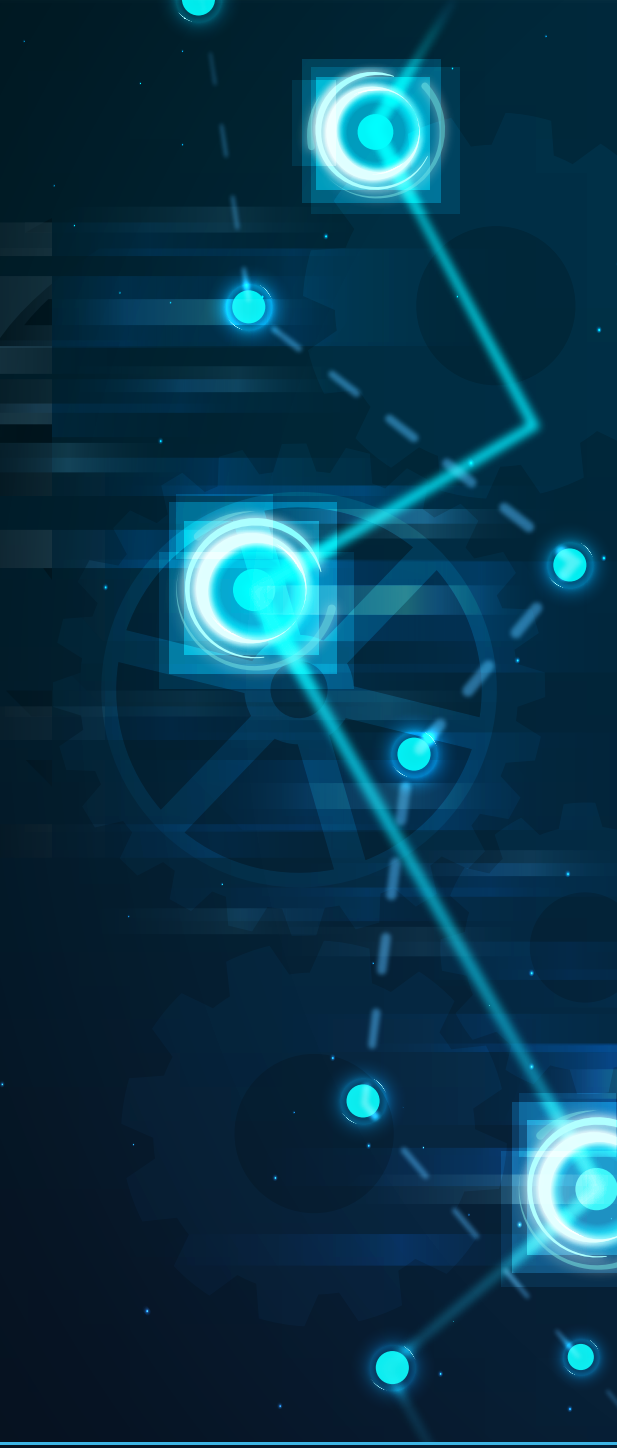
It requires a multi-layered strategy which encourages firms to move beyond strict threat prevention and to incorporate technologies that can mitigate the damage from sophisticated cyber threats like ransomware and recover data quickly after an attack.

Steps to Enhance Cyber Resilience

Firstly, every business must understand what its DNA is — that's the critical 10%-15% of data and mission critical business applications that must be protected at all costs.

The next step is to explore a more resilient infrastructure than solely back-up environments to protect an organisation's data. This process can be simplified and made more effective by services that enable organisations to move business critical data into an isolated air gap environment and lock it down in less than five steps.

This is what we call a cyber vault. This provides the ultimate protection for businesses critical information. In the event of an attack, this data will help businesses to



recover. A true logical air gap needs to be inaccessible and offline, not just in a different location. Otherwise, it can still be compromised by cyber criminals. Under this model, a firm's data is online for an hour every few days at most.

From engaging business leaders and from the results of Dell's latest Cyber Resilience Survey, it is clear that many struggle to differentiate cyber protection and data protection as well as data backup versus recovery.

Through its advisory services and cyber recovery solutions, Dell has been enabling some of Ireland's leading businesses to not only navigate the ever-changing cyber landscape, but also to more easily achieve cyber resilience as they continue to transform at speed.

Looking Ahead

As we look ahead, one thing is certain, businesses and organisations will handle more data than ever before. That's why it's critical that leaders review their data protection strategy to ensure they can secure and protect data irrespective of where it is located within their organisation.

Organisations can no longer simply focus on just protecting individual IT systems or devices — they need to assess the ability of their entire business to withstand and recover from a cyber-attack.

At Dell, we've been helping companies to strengthen their cyber resilience, so they have a secure foundation on which to grow and innovate. With seven-in-10 companies in Ireland accelerating their digital transformation plans, business resilience will increasingly be tied to cyber resilience.

FURTHER INFORMATION

For futher information, contact Dell Technologies Ireland:

Lisa Holmes, Marketing Manager, Dell Technologies Ireland.

Email: lisa.holmes@dell.com

Website: www.delltechnologies.ie