Data Privacy Day

Millions of people are unaware of and uninformed about how their personal information is being used, collected or shared in our digital society. Data Privacy Day is an international effort to empower individuals and business to respect privacy, safeguard data and enable trust.

Significant losses

Over the last few years, businesses have been increasingly impacted by the rise in cyber and data crime, with:

Four in ten

Four in ten businesses (39%) report having cyber security breaches or attacks in the last 12 months.

181 days

Organisations in the UK taking an average of 181 days to identify the fact that a breach had occurred, and a further 75 days to contain the incident.

£2Bn

Losses to fraud and cyber crime in the UK totalled almost £2 billion in 2020

Growing importance for business leaders

Business leaders understand that with the rise in cyber threats, more needs to be done to prioritise cyber security within their business, with:

55% — 55% of businesses planning to implement a cyber security training and testing programme for all employees within the next two years.

40% — 40% of business leaders not being confident that people in their business would know how to spot a cybersecurity risk.

77% — Three-quarters (77%) of businesses saying cyber security is a high priority for their directors or senior managers.

Click **here** to read more insights in Distology's full report – The Future of Cybersecurity 2022 & Beyond.

Steps businesses can take

1

Many organisations are using dated technology that isn't capable of protecting them from the increasing cyber risk. In a time where remote working has never been more prevalent, organisations need to be prioritising and analysing their cyber security approach, tools and technologies to ensure they are up to date and leaving no gaps for attackers

2

Whilst implementing preventative solutions can help to keep threats locked out for longer, it's inevitable that breaches will happen. The next step is to think about identity based encryption solutions which can ensure that any information that is discovered, is only useable and legible to those with the 'keys' to unlock it.

3

Finally, you can have the best solutions in place, but people will always continue to be the weakest point in the chain of defence. There are a number of ways employees can fall victim to a security breach, that could have a detrimental (not to mention costly) impact on the organisation. Training your employees to understand the cybersecurity risks and spot potential security breaches/attacks should be prioritised.

Distology.

NorthEdge portfolio company Distology is a value-added-distributor representing vendors of IT security technology products across EMEA, helping to protect businesses' digital estates from the growing threat of cyber-attacks. Their Chief Product Officer shared their thoughts with us on the importance of education and working together to secure our lives in the most effective way.

> **"We've seen an incredible amount of innovation from businesses over the past two years as they have evolved to ensure business continuity through remote working technologies and e-commerce platform to meet customer demand. However, this agility comes with the increased risk of cyber threats, as attackers are using smarter techniques to target vulnerable businesses. Whilst businesses can take pro-active steps to understand where the major risks are and decide upon sensible mitigation moves, it's also important to remember that many businesses are not alone in the uphill struggle to secure their organisation. To secure our lives as best as possible, we need to work together, as peers, to educate each other on what solutions could be adopted, with a view to select the right ones that should be adopted, to find the right blend of cybersecurity defences, detectors and responses for each organisation."**
>
> Lance Williams, Chief Product Officer

How we support our portfolio

At NorthEdge we take our responsibilities as investors and employers seriously. We support our portfolio companies throughout the investment cycle to mitigate their risk of cyber-attacks and effectively manage their cyber security response through a programme run by a specialist third-party operating partner. We encourage sharing of best practice through our dedicated operating platform and share regular insights from specialists in our network.

Click here to find out more about how we integrate all elements of ESG into the Value Creation Plan.