Angela Madden, managing director, RITS Information Services
Picture: Maura Hickey

while the other is exploratory and experimental.

Marc O'Regan, chief technical officer of Dell EMC, sees this approach as necessary to the current state of cloud. "Dell Technologies takes a very very open, pragmatic view of cloud. We see cloud as an operating model, rather than a place."

O'Regan views cloud security as pivotal to the process of digital transformation, or, as it is beginning to be called within Dell EMC, 'innovation transformation'.

"IT transformation brings its own risks. Security transformation means looking at end points, IoT, things like neural nets, computational algorithms, speech recognition, chat bots or very tight security products," he said.

This means fostering a forward-looking culture which supports ideas and innovation, while putting equal resources into protecting what's already there. "When I talk about digital transformation, I see it as an umbrella term describing IT transformation, workforce transformation and security transformation," O'Regan said.

"Any control system is within the heart of the data centre, and then permeates out to the different areas of the business in order to protect them. This is a big challenge for industry when we try to articulate what Gartner brought to us four or five years ago, the idea of bimodal IT. It means securing what we have right now from a traditional perspective, but also exploring areas like IoT and edge devices, and other new sources we've not looked at before."

In choosing a cloud provider, CIOs and the organisations they're part of need to be cognisant of the future, as well as their current security capabilities: "This moves from a maturity discussion into a platforms discussion . . . The problem organisations try to grapple with more and more, as I see it, is choice around those providers, and understanding which providers can give them the mechanisms, modes and models they need in order to compute in a confident way on a platform of choice."

Andrew Philpott, VP of EMEA Sales at Bitdefender, stressed the importance of working out the specifics of access up ahead. "Clients are individually responsible for securing their workloads," he said. "Organisations should start with implementing access, authentication, and accounting controls for limiting potential unauthorised access to sensitive data, they should understand where their data resides and how it's stored (encrypted or unencrypted), and also deploy EDR and security solutions that are virtualisation-friendly."

The trick is to make attacking your data difficult enough that it's not worth the criminal's time: "Ultimately, increasing the cost of attack for cybercriminals is the best approach, and when building an effective cloud security strategy organisations need to factor in how important is the data they're handing versus the potential impact of a security breach on their business continuity."

Automation has already dramatically changed cloud security for the better. A new wave of endpoint detection and response tools can automatically root out threats and resolve them, freeing up IT and security teams to focus on relevant and timely action. Philpott said: "The use of machine learning to augment EDR solutions to remove alert fatigue is probably the most dramatic change in the way organisations can approach visibility into their infrastructure without sacrificing time, increasing budgets for personnel and ensuring timely incident and response capabilities."

In the wake of GDPR, these methods are more crucial than ever. "GDPR has placed a lot of focus on data and how security should revolve around securing it. However, the fact that organisations need to have an incident response plan and report data breaches within 72 hours – or else risk being significantly fined – has proven an effective incentive for increasing visibility by integrating EDR tools with existing layered security solutions," Philpott added.

For most organisations, the advantages of cloud continue to outweigh the risks. "It is all eggs in one basket, but the basket is a lot easier to protect," Conway said. "Even from the point of view of reliability, a data centre that's well protected will have fire protection, detection, sensors, stand-by generators, and a whole range of security measures, while if you're storing your data on a server in house it'll be in the corner of the office gathering dust."

Madden added: "For larger organisations, in particular SMEs, it can be very expensive to have a security person full-time. Going to the cloud can be beneficial. With continuity as service, as one examples, they're built up in terms of not only environmental controls, but also resilience. Often they have multiple data centres, so that if one were to fail, it would automatically move data to another data centre. That level of backup would be too expensive to do internally."

"As we look at workforce transformation, educating our workforce and making them more aware of their responsibility to their environment is more and more important. If you talk to any organisation and ask them what the biggest risk factor is, they'll tell you it's people, whether that's inside the organisation or outside it. Humans are a massive risk," O'Regan said.

Is your business cyber-ready? A new report from Vodafone

Dr Csaba Kiss Kalló, head of portfolio in connectivity, mobility and security at Vodafone

The results are in, and less than one-third of businesses feel that they're ready for the future. At least, this is what Vodafone's newly-published Cyber Readiness Barometer indicates. Intended as an insight into how businesses approach technology in six categories – operations, resilience, digital footprint, strategy, awareness and risk – the survey was conducted on 1,528 business and IT decision-makers in nine different countries, with 99 of them coming from Ireland.

"Data breaches are a growing tendency, in a large part because cloud users assume that their data in the cloud is fully secured by the cloud service provider," said Dr Csaba Kiss Kalló, head of portfolio in connectivity, mobility and security at Vodafone. "Education is the least cyber-ready industry, while the healthcare, technology and financial services sectors are the most prepared."

The report indicates a lack of confidence and, more critically, a lack of preparation for regulatory chances which have already been implemented. Only 43 per cent of respondents surveyed in April 2018 said that they were aware of and had taken measures to comply with GDPR. The highest awareness was among technology and media companies (78 per cent), where 54 per cent of respondents had also taken action to comply. Kalló commented on the large number of post-GDPR emails, pop-up windows and cookies asking permission for information.

"We normally like to just conveniently hit okay on these requests, but if we inspect the details closer, we sometimes discover that we are giving permission for our details to be used in hundreds of different contexts and third party organisations. I hope that the Data Protection Commissioner's office is closely watching this new approach to getting access to personal data to make sure that the purpose of GDPR is not weakened," he said.

While many organisations are still catching up in the wake of GDPR, Kalló has noticed that cloud security is receiving more attention. "Investments in cloud security are proportional with other cyber security investments, which in general are increasing due to the recent highly mediatised attacks, as well as due to fear from potential reputational damage," he said.

If your business does get attacked, it's important to respond quickly and efficiently to contain the threat. "The speed of reaction to an identified attack is critical for minimising the damage," said Kalló. "At this phase automation is very valuable for distributing protective measures for stopping the attack."

Already, cloud security vendors are putting these automated tools into action, learning patterns of behaviour and events within the systems they protect. "They can then spot deviations from the 'normal' patterns and initiate action if an attack is in progress. AI is also used to collecting security intelligence from across the internet proactively and aid in speedy identification of threats. AI-based automation technologies are currently at the beginning of their maturity curve."

Another area currently in development is edge computing, fuelled by 5G and the demand for low-latency applications. Kalló said: "The basic concept of edge computing is to create a distributed cloud where small regional interconnected data centres serve local applications. This enables significantly lower service latencies necessary for certain applications such as AR (augmented reality), robotics, connected cars, industrial machinery control." However, network architects will need to work closely with security experts in order to build in 'protection by design'.

"Such distributed edge data centres and the new applications come with their own security challenges, such as an increased attack surface, system safety, long lifespan of embedded technology and multi-vendor software environments."