



RESILIENCE FIRST

SURVIVE & THRIVE

Resilience First Webinar Summary

'Digital Resilience – challenges and opportunities'

In collaboration with Accenture

Chair:

Heather Adams, Managing Director, UKI Risk Strategy and Consulting Lead, Accenture

Speakers:

Professor Weisi Guo, Director of the Smart Living Grand Challenge and Head of Human Machine Intelligence Group, Cranfield University

Carl Dukatz, Global Lead of the Quantum Computing Program, Accenture

Hamish Wynn, Managing Director and Leader within Digital Risk, Operational Resilience and Cloud Transformation, Accenture

Nigel Sutton, Digital Rail, Thales Ground Transportation Systems

In brief

Already underway, the 4th Industrial Revolution is a development that is characterised by a fusion of technologies that blur the lines between the physical, digital, and biological spheres. When compared with previous industrial revolutions, the 4th is moving at an exponential rather than a linear pace. Moreover, it is both advancing and disrupting almost every industry in every country. The breadth and depth of these changes herald the transformation of entire systems of production, management, and governance.

This webinar looked at three digital technologies that are expected to bring about fundamental change, namely Artificial Intelligence, Quantum Technology, and Cloud Computing. Experts in their respective fields explained and discussed the challenges and opportunities in these exciting new subjects. The webinar presaged the launch of a [whitepaper on Digital Resilience](#),

The event and paper were produced in collaboration with Accenture and Cranfield University.

Introduction by Chair

Following remarks by Mike Rooney on behalf of Resilience First, **Heather Adams, Managing Director at Accenture** set the scene for the remainder of the event.

She explained that resilience was the ability to cope with shocks and stresses and be able to bounce back. Concerns about the resilience of digital systems are not new and advancing technology and the interplay between technologies makes it even more challenging. More positively, though, technology can also enhance resilience. She gave examples of access controls to cloud computing and guidance available to businesses to help protect system design and described how we would look in more detail at the opportunities that digital brings in this webinar and in the accompanying report. Heather invited each speaker to give a brief overview of their knowledge of the technologies now available.

Artificial Intelligence (AI)

The core concept of AI, namely the ability of machines to learn and exhibit human-level intelligence, remains unchanged. However, the past decade has witnessed an astounding growth of AI innovations and applications. AI generally refers to a combination of technologies that is capable of acquiring adaptive predictive power through some degree of learning from data and task information.

Often this is real-time at a scale that would otherwise require significant human resource. For example, by scanning satellite imagery or extensive network databases. AI can make complex decisions faster, for example, in an automotive vehicle or in personal product decisions. More recent advances, such as fake profiling can be used both positively, to aid, and negatively, to disrupt. The democratisation of access to technology allows increasingly low skill business access.

AI comes with its own risks to business, such as greater dependency on high skill engineers for insertion and implementation, and retaining and training of suitably qualified persons particularly in such a fast-moving and fluid environment. AI is also open to adversarial attack by vectors which can operate by themselves or operate in combination with more conventional cyber-attack. Trust between AI and human interaction is needed for effective collaboration and legal and policy frameworks assist in this regard.

Quantum technology

Quantum technology can take three different forms – computing, sensors, and communications. All share the same physics. These new technologies can have the potential to transform businesses by creating solutions for problems that were previously thought insolvable.

Quantum computing allows more advanced operations than can be realised on classical computers, particularly around protection using quantum error correcting codes. When combined with aspects available through cloud computing, resilience can be greatly enhanced. Machine learning, too, can enhance resilience, for example, by identifying certain types of cyber-attack and blocking these whilst legitimate traffic is still allowed to flow.

Quantum sensors offer enhanced ways to observe and measure physical properties such as gravity and light. This makes them particularly good at active and passive resilience and able to identify specific environmental conditions in early warning systems to protect against natural disaster impact.

Quantum communication methods are known to be more secure than classical encryption and this is particularly useful as an active resilience tool in identifying and addressing attacks on a communications system.

A businesses' system can be enhanced by combining all three forms. It is still early days for quantum technology, but continued growth and further new uses are anticipated. The technology is used with both cloud computing and AI. The former as the primary access means and to reduce cost and the latter to access more datasets which enhance the useability of the technology.

Cloud Computing

The journey to digital and the associated cloud transformations are not brand new and while some organisations have already begun the ride others are just starting. With the speed provided by the cloud, and by working with Cloud Service Providers, enterprises can shift away from operations aimed at keeping the lights on, freeing up their budgets and their teams' time to rethink fundamentally how the business operates, and how it creates value. This is the ultimate objective of a cloud journey – to create a platform for innovation, agility, and future business.

The cloud can be public, private or, indeed, a hybrid. Private being owned and maintained by a single organisation. Resilience in the cloud must be strategically planned and intentionally implemented. Governance and control are necessary to manage risk in cloud use and regulatory scrutiny may make this imperative in order to demonstrate management. Testing is still fundamental in the move towards cloud migration, this includes resiliency testing.

In summary, cloud computing is critical for digital resiliency, and acts as a catalyst for digital modernisation for many businesses.

What does this mean for businesses?

Each of the above technologies has their own risks and businesses need to be aware of these to effectively manage the use of new technology.

Starting with AI:

- There may be regulatory or ethical issues and some of the AI being produced may not have ethical outcomes
- How will a business know what the risks of a particular AI are and whether it is a current risk or whether it is tolerant or not? Indeed, several variables can exist in usage which can confound evidence, e.g. imagery from AI at night may have different outcome to that used during the day
- Understanding adversarial vulnerability is important as AI use by business increases

For quantum:

- Sabotage or government espionage is an issue in the short term
- In the medium term, affordability of quantum technology may open this to greater access by organised crime
- Businesses need to be aware of these risks and have an IT resource that can manage these

- Businesses should start using quantum technology as early as possible. Is it estimated that if a business doesn't start building its quantum resilience now then it may never be able to catch up

For cloud computing:

- New legislation, e.g. for data protection and data security, cyber security, covers cloud use. Legislation covers not only the UK, but the EU, and US have developed similar rules.
- Cloud carries security risk and the risk from cloud needs to be mitigated down to an acceptable level. This can be bespoke depending on the business or its size or sector or how data is hosted

What impact has the COVID pandemic had on the digital revolution?

- This has presented greater degree of opportunity. Not only for consumers and business providing to the public but, for example, includes drug research and in the optimisation of medicine supply chains
- It is important to learn from the operational disruption during the pandemic as this will be valuable during future shocks
- Digitalisation helped us to get through the pandemic – compare this to how we might have coped before we had modern digital capability

How can business innovate and embrace the new technology safely?

- Businesses need the right level of security and technology in place. Equally important, a business needs the right governance and independent scrutiny of its technology systems, i.e. not have those building controls also checking them
- Mentality of the business is important – some are more up for new technology. Businesses need to be aware of the challenges and of regulatory and legal frameworks and of the technical challenges they may face, i.e. be prepared and do some research on your system first

Please [click here](#) for a copy of the webinar recording and [here](#) for a copy of Resilience First's Digital Resilience Report, in collaboration with Accenture and Cranfield University.

Speakers' Biographies:

Heather Adams

Heather Adams is Accenture's Managing Director, UKI Risk Strategy and Consulting Lead. She is passionate about working with clients across sectors to build resilience. Over 23 years in consulting she has worked with senior leaders to define and deliver their resilience, risk, and compliance strategies. She has experience of working across business and technology functions to deliver strategic change programmes globally. Typically, she crafts and delivers solutions that are innovative, data-driven and that leverage new technologies to drive effectiveness and efficiency

Professor Weisi Guo

Professor Guo leads the Cranfield University Grand Challenge of Smart Living and his own Human Machine Intelligence research group. He graduated in MEng, MA, and PhD from Cambridge, and was a Turing Fellow at the Alan Turing Institute. He has been investigator on over £16m of government research grants in machine learning, resilience, and 5G networks. He is known for his work in using AI to forecast conflict (Nature'18) and geomagnetic storms (Nature Comms.'21), developing green AI (Nature Comp. Science'21), and developing bioengineered information systems. He now works to develop trustworthy AI for future autonomy, and runs a MSc in Applied AI to up-skill engineers

Carl Dukatz

Carl is the Global Lead of the Quantum Computing Program at Accenture. Over the past five years he has led the creation of dozens of quantum applications and prototypes, published research and business perspectives on quantum, and developed multiple training and workforce readiness programs for quantum practitioners. Today, Carl focuses on helping businesses map their most challenging problems to formulations that will one day run more efficiently on quantum computers

Hamish Wynn

Hamish is the Managing Director and Leader within Digital Risk, Operational Resilience and Cloud Transformation within Accenture's Regulatory and Compliance practice. Hamish has a focus on Operational Resiliency and is actively engaged within industry efforts. Hamish has extensive risk and regulatory change management experience, and partners with top tier Global Financial Services organizations to help transform their business and expand the partnership with Accenture in key areas. Hamish has over 18 years industry and consulting experience. Hamish holds a Ph.D. in Chemistry from the University of Cambridge and is based in New York

Nigel Sutton

Nigel is a client facing security architecture consultant. He has strong understanding of the underlying technologies, is very much focused on Business outcomes to enable the Business need, while ensuring solutions and services meet legislative and regulatory obligations with appropriate cost-effective security controls to ensure that both the risk appetite and business requirements unite to deliver an adequate secure solution, which allows Accreditation/Certification/Assurance to be achieved

Michael Rooney

Mike was previously the Chief Operating Officer of London First (2004-2018) and was responsible for member management, commercial development, and company support services. Before joining London First in 2002 as Commercial Director, he was Chairman and Chief Executive of Langdon's Foods Plc. He has had a wide experience of the dairy industry having worked during the 1980s and 1990s in senior management positions for Dairy Crest Foods Plc and as Household Director responsible for the doorstep delivery business. His early career was spent in marketing and advertising, working with leading advertising agencies including CDP and Inter Public as an account manager