JULY 2018

WHITE PAPER

Digital Resilience

UNDERSTANDING THE CHALLENGES OF RESILIENCE IN DIGITAL ENVIRONMENTS

Institute for Strategy Resilience & Security
University College London

UCL

in association with

Shearwater Group

Forewords

The Rt Hon. Lord Reid of Cardowan
Executive Chairman, ISRS

Since its foundation, ISRS has focused on addressing complex, existential challenges within government, business and the public sector. Today we are witnessing an inexorable and accelerating shift towards a pervasively interlinked world of systems and supply chains that touch virtually every aspect of our lives. Goods, services, people, organisations and information are becoming globally interconnected and accessible in ways that were previously unimaginable. We are merely at the start of this digital journey – emergent fields such as machine learning and quantum computing will advance, combine and be applied in ways that will render today's technologies as antiquated as a manual typewriter.

Immersion in this digital environment presents organisations with the strategic imperative to generate value and take advantage of an unparalleled abundance of new opportunities. Yet increased reliance and the expectation of continuous availability come at a price, predicating operations on the assumption that underlying systems will always be present and functional. This white paper attempts to draw out some of the most important issues of both opportunity and risk, and illustrates the need for consideration of *digital resilience* at the most senior levels. I believe that there has never been a more important time to do so.

Michael "Mo" Stevens
CEO, Shearwater Group PLC

In 2016, Shearwater Group agreed its transformation strategy to build a leading UK based digital resilience group. This forward-thinking strategy was designed to address the complexities and challenges of the future that enterprises will need to meet if they are to survive, evolve and succeed in the expanding global digital business environment.

We see that many enterprises have yet to move beyond a traditional, defensive "lock-down" approach to corporate perimeters, or to embrace the ongoing viability and vitality of their enterprise within the context of customers, suppliers and partners. Cyber security has at last been elevated to the boardroom, however, business resilience remains poorly understood, with digital resilience in particular, seen only as a property of the strength of an IT system's security.

This traditional approach fails to recognise digital resilience as an enabler of today's entrepreneurial and fast-moving digital business environment, and the resultant competitive advantage it brings. Digital resilience is the very foundation of the modern business and should be recognised as the most valuable long-term property of an organisation.

We are delighted to have supported the development of this white paper by ISRS, which sets out a framework for the challenges of a new generation of leadership thinking in the digital environment. As we stay abreast of the ever-changing digital business environment, we look forward to building on the frameworks, challenges and questions presented and to participating in many further discussions with the business community that we serve.

Institute for Strategy Resilience & Security
University College London

Shearwater Group

Contents

TO DOWNLOAD YOUR DIGITAL COPY OF THIS WHITE PAPER AND HELP SHAPE WHAT NEEDS TO HAPPEN NEXT, PLEASE REGISTER YOUR INTEREST AT

www.digital-resilience.com

About Shearwater Group plc

Shearwater Group plc (www.theshearwatergroup.co.uk) is an AIM-listed company (LON: SWG) focused on building a UK based group providing digital resilience solutions. Our aim is to acquire and develop information, security and cyber security companies with a leading product, solution or service capability whose full potential can be unlocked through active management and capital investment. We will deploy a 'buy, focus, grow' strategy to deliver enhanced value through our acquisitions and help to solve the core scaling issues faced by SME information, security and cyber security companies.

About the Institute for Strategy, Resilience & Security (ISRS) at UCL

Over the last decade the Institute for Strategy Resilience & Security (ISRS) at UCL (www.isrs.org.uk) has served as a pioneer and forum for next generation thinking. Founded by the Rt Hon. Lord Reid of Cardowan, ISRS provides analysis and assessment of the major issues of resilience with respect to national and global infrastructure and the ability of governments, regulators and businesses to respond to them. The Institute advises industry and the public sector on the persistent challenges to their agility, stamina and capacity in strategic decision making, so as to better face existential threats, risks, and disruptive innovation that are not addressed by conventional strategy and forecasting.

For industry and public sector queries in relation to this paper, please email: info@isrs.org.uk

For media enquiries about this paper, please email: press@isrs.org.uk

ISRS would like to thank the many contributors to this white paper and in particular:

The Rt Hon Lord Reid of Cardowan, Chris Hurran OBE, Air Cdre Bruce Wynn OBE, Prof JP MacIntosh, Peter Domican, Asutosh Yagnik, Mark Child, Paul Kenealy and David Levinger.

7 KEY TAKE HOME MESSAGES *FOR SENIOR EXECUTIVES*

1. **Digital resilience is about the resilience of your organisation and its business processes in an all-pervasive digital environment, not the resilience of your IT function**. Organisations must acquire a dynamic state of continual evolution and learning and the capability to use new challenges not merely to rebound but to bounce forward -- crises become pointers towards opportunity and catalysts for evolution.

2. **Digital resilience is one of the most valuable long-term properties of your organisation and it must be managed at senior leadership level, and understood throughout the entire organisation, as both a business and a technical matter.** It must not be conflated with cybersecurity or disaster recovery. It defines your capabilities for forward evolution and survival in the light of a changing environment, through the successful implementation of an evolving business strategy.

3. **The core business processes of most firms and 100% of digitally native businesses are now entirely dependent upon digital technology.** Reversionary modes of operation, for example, switching to processes that are less dependent upon technology, are often no longer possible in the event of disruption or failure. If your assessment is that significant digital disruption may disable your core business processes, then digital resilience has become tantamount to business resilience.

4. **Digital resilience is about opportunity and risk in equal measure, with new technologies generate novel modes of both resilience and irresilience.** Equally a failure to adopt new technology that delivers superior customer value leads to poor competitiveness versus more nimble rivals is a resilience issue as a determinant of business survival or failure.

5. **More secure does not mean more resilient.** While a less secure technology solution may pose access vulnerabilities, a more secure solution may introduce flawed assumptions, irresilient processes or lead to catastrophic business inflexibility. Any new digital infrastructure must therefore be assessed in terms of its overall impact on business resilience, both in terms of opportunity and risk.

6. **The networked interactions of processes, people and technologies generate complex non-deterministic, emergent and unforeseen resilience vulnerabilities.** In a fully connected environment, the more tightly coupled, rapid, and efficient digital processes are during normal operation, the more disruption poses a threat and the greater the risk that cascading failure will render core processes inoperable.

7. **Digital resilience requires a fundamental shift in how you manage both risk and opportunity.** Traditional models of atomised risk mitigation and impact analysis are no longer sufficient. Digital resilience must be assessed in terms of combinations of long-tail effects and capabilities to anticipate, respond, learn and evolve appropriately to shifts in a hyper-networked digital environment. Digital resilience thinking ensures that the entire organisation is considered and challenged in the light of enabling and balancing growth, evolutionary change and security needs appropriately.

Institute for Strategy Resilience & Security
University College London

Shearwater Group

A Digital Resilience Leadership Checklist

An assessment framework of key questions for leaders to define, identify and address digital resilience issues within their organisations

1. Is digital resilience understood at a senior level?

- Do we understand what digital resilience means and how it differs from cybersecurity?
- Do we fully appreciate how dependent our organisation is upon digital technology?
- Are we sufficiently aware of the opportunities and risks of our digital environment?

2. Is digital resilience a leadership or an IT issue?

- Is resilience discussed within our leadership team or do we treat it as a separate IT, cybersecurity or risk register issue?
- Does our organisation's leadership encourage and empower senior individuals to critically discuss existential threats?
- Is our board aware of the potential impacts of irresilience and does it have digital processes in place to address them?

3. Do we understand how critical digital resilience is to our business?

- Is our level of resilience appropriate for our organisation?
- Have we reviewed the level of irresilience that we are willing to accept?
- Have we assessed our capacity to innovate and adopt innovation?

4. Have we assessed our digital resilience exposure?

- Have we assessed the ways by which digital irresilience may result in harm to our business model, processes, people?
- Have we worked through potential consequences and built scenarios for how these may evolve?
- Have we mapped the interactions of our risks and vulnerabilities, or are we treating them as isolated?

5. Do we have an active programme to build and embed digital resilience thinking and practice throughout our organisation?

- Are we actively building resilience for both business process, existing digital infrastructure and new infrastructure?
- Are we putting in place processes to encourage adaptive behaviour, continual evolution and learning environment?

Digital Resilience

The power of an organisation and its business processes for recovery, renewal and evolutionary transformation, in an all-pervasive digital environment

Institute for Strategy Resilience & Security
University College London

Shearwater Group

EXECUTIVE SUMMARY

What Is Digital Resilience?

Digital technology has become a vital infrastructure underpinning the functioning of every aspect of human society, increasingly interwoven with decision making and business processes. We are approaching near total reliance. When a human, however capable, is unable to substitute for a digital process, it can be said to be fully digitally dependent and its business resilience is now an issue of *digital resilience*.

Opportunity And Risk In Equal Measure

Resilience thinking encompasses both opportunity and risk in equal measure. Failures of imagination by organisations to address the opportunities that emerge from the digital environment represent potent catalysts of future existential crises.

Kodak ignored the pace of development of digital photography and mobile phones with dire consequences. Within a decade it had gone from a technology leader to bankrupt, and was virtually irrelevant to the industry that it had once dominated. While the lessons of this classic business failure have been widely reviewed, businesses today remain as prone to these vulnerabilities as ever. An existential crisis is underway in the retail sector as traditional high-street players have failed to develop effective competition in an e-commerce environment. Burdened with the cost base of physical assets, unlike their digitally native competitors, their technology footprint is not one of rational design, rather the result of many incremental and disparate decisions.

Facing a digitally dependent future, CEOs and their boards need to take a more direct interest in digital resilience. They must ensure that their organisations identify current digital resilience deficiencies not just through cybersecurity and risk functional specialisms, but through embedding a resilient approach and culture.

Digital resilience is about acquiring a dynamic state of continual evolution and learning within the digital environment. When fully understood and implemented, digital resilience should enable an organisation to be able to use new challenges not merely to rebound but to bounce forward, with crises becoming pointers towards opportunity and catalysts for evolution.

Cyber security, disaster recovery, business continuity and back-up are important sub-components of resilience implementation, yet while defences provide protection, they may also be a source of irresilience. It is intuitively tempting to view security as promoting resilience, but it is important to consider that although a less secure technology solution may pose vulnerabilities, a more secure solution may introduce flawed assumptions, irresilient processes or lead to catastrophic business inflexibility, by locking business processes into digital dependency.

Except in the most restrictive cases, digital environments are now permeated by a myriad of devices and digital services that transcend traditional hierarchical relationships. The notion of a defensible, well defined perimeter has been replaced by the need for a holistic approach to digital resilience that encompasses the complex graph of interactions between employees, contractors, suppliers, partners, customers and digital services. Each individual entity, whether human, hardware or software is embedded within the graph of their digital tribe, enterprise, nation and planet. Increasing interconnection raises the likelihood and impact of risks to resilience as any underlying single node may extend and cascade vulnerabilities across the entire network. Given a surging Application Programming Interface (API) economy with currently more than 17,000 web APIs and a forecast of over 20bn connected devices by 2020 , the "Internet of Things" (IoT) and the "Industrial Internet of Things" (IIoT) pose significant resilience challenges[1,2].

A Strategic Approach To Digital Resilience

Implemented strategies and solutions must be engineered in the knowledge that the challenges and opportunities arising from digital resilience will change constantly. There is no going back -- the alternative is to continue pre-digital management practices in a digital environment at the risk of existential failure.

We look to define the principles of a strategic process to identify digital resilience issues both from a business and technology perspective and address them through the development of organisational capabilities. Digital resilience must be assessed and mitigated in terms of the capability to anticipate, respond, learn and evolve.

Introducing Digital Resilience

- Most organisations have not fully grasped the extent of their dependency upon digital technology.
- Digital resilience requires total awareness of the opportunities and risks of the digital environment.
- Cybersecurity is a important subcomponent of digital resilience, but they are not the same thing.

As we head towards a future operating environment where virtually every business model and process is fully digitally dependent, we observe that many organisations have yet to accept and internalise the degree to which their operational resilience is coincident with digital resilience.

Digital resilience thinking encompasses both opportunity and risk in equal measure in the new digital environment. Disruptive technology has the ability to change the entire competitive landscape, so failures of imagination by organisations to address emerging opportunities may represent potent competitive risks. Those unable to anticipate and drive change fast enough within an appropriate time-frame may find themselves in existential crisis. Yet the same pressures of hyper-competition for the utility and efficiency provided by digital business models, mean that keeping pace may be at odds with the resilience issues of technology.

With the potential for failure of any critical technology component, either through malfunction or uncompetitive function, to trigger financial and reputational crisis, we propose that this issue demands a new focus from the Chief Executive Officer and the Board. The majority of large businesses produce strategies with a 3-5 year outlook, too short a time period over which to completely re-engineer operating models and organisational competencies. Leadership teams need to consider their resilience within the digital landscape outside of their conventional analytic window and be prepared to make major changes to adapt, both to new threats and opportunities at a relevant pace. What is ostensibly a technology choice is now an issue of existential importance, balancing the opportunities for commercial advantage and cost saving with the networking of risk i.e. a lack of reversionary modes and potential losses in the event of a major outage, quite possibly entirely outside of the control of the company itself.

Resilience in a Digital Age

Resilience is one of the most valuable long-term properties of an organisation, defining its capabilities for forward evolution and survival in the light of a changing environment, through the successful implementation of an evolving strategy. As crises are often driven by events that are beyond control, resilient organisations are those who are prepared to anticipate and face these challenges head-on, then through adaptation, emerge with increased competitive advantage in a new state and context.

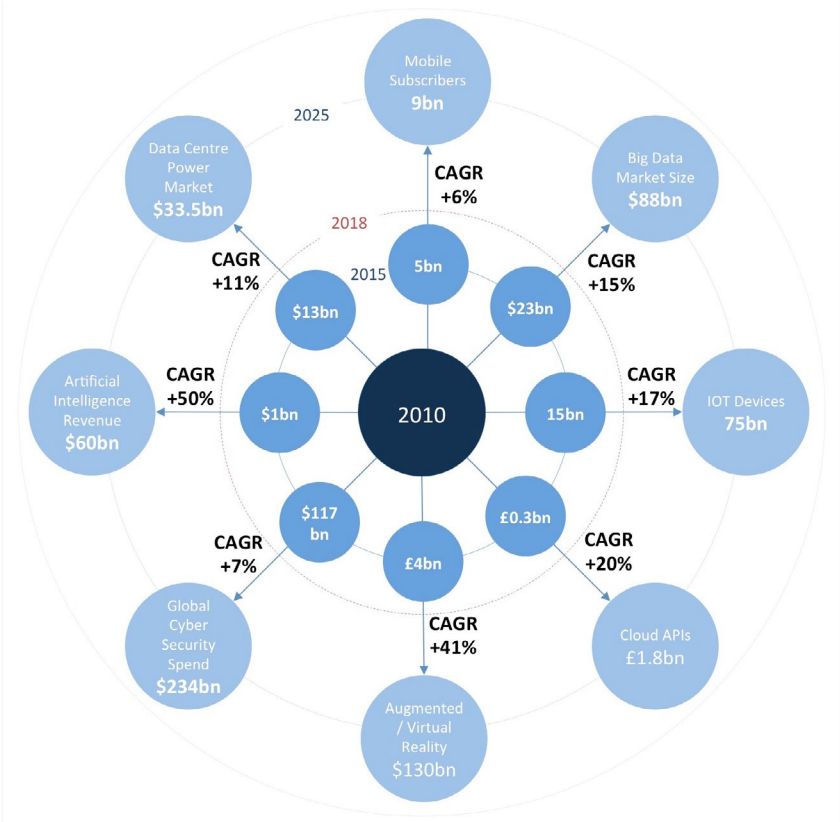
The Digital Revolution is rapidly transforming the way our cities, homes, workplaces and public services operate with pervasive technology. We are witnessing the inception of the 'Internet of Things (IoT)' and 'Industrial Internet of Things (IIoT)', where virtually every physical object becomes a networked device, empowered with sensors, intelligence and the ability to

Institute for Strategy Resilience & Security
University College London

Shearwater Group

FIGURE 1

Growth forecasts suggest further acceleration of the pace of digital technology adoption, with full global reach being achieved within the next decade [7].



communicate. It is clear from growth forecasts of underlying trends (Fig. 1) that we are merely at the dawn of this development.

Having replaced human hands, the combination and compounding of technologies portends a future that will be orders of magnitude more technologically enabled and sophisticated than today. Machine intelligence is increasingly replacing human brains, with decisions taken and business functions operating with ever greater autonomy. Deterministic systems are giving way to an acceptance of "black box" intelligence, where neither the rationale nor the decisions, are necessarily open to human analysis or comprehension, even by the software engineers who create them. Systems now commonly contain millions or even billions of lines of code, that are both being continually updated and linked to other changing digital services. Multiple versions of the same software may exist simultaneously, as users fall out of sync with each other and companies test different product features. The state of the collective system at any point in time is no longer a defined function of the code and the outputs empirical in nature.

Towards Total Digital Dependency

The effect of the Digital Revolution upon organisations has already been profound. From an earlier model of "IT" as a decision support function, core business processes that now interwoven with their underlying technologies. In the case of digitally native companies, such as search and digital services giant Google, the entire operating model is inseparable from and synonymous

Defining "Total digital dependency"

Dependence of core operational processes on digital technology, such that the failure of these systems and the loss of their information creates an immediate inability of the organisation to function effectively, and where a prolonged outage may pose an existential threat.

The core business processes of most firms (and 100% of digitally native businesses) are now entirely dependent upon digital technology to the extent that reversionary modes of operation are no longer possible in the event of disruption or failure.

ISRS defines a reversionary mode as the ability of a body to move to a contingency mode of operating, within a time framework that enables the task to be resumed to a comparable degree of efficiency and without significant inconvenience to the user.

with the technologies that support it.

Digital services are increasingly being produced and consumed as though they were "always on" utilities, yet often with no functional alternatives. Historically, in the event of failure, discrete processes coupled together by human flexibility could be temporarily substituted by alternate technologies, or if necessary, by a manual process. However, where digital services are tightly integrated, reverting to an earlier version of a component technology may no longer be possible. Interfaces and other dependencies may have become incompatible, and no human, however capable, can substitute for the complex automation contained within the digital work-flow. Furthermore, the higher the quality of service that is assumed to be provided under normal circumstances, the greater the potential for digital *irresilience* when this is no longer the case.

A recent study by Lloyd's of London, in conjunction with risk modeller AIR Worldwide[3], modelled the expected financial impact on 12.4 million businesses in the US in the event of a major prolonged cloud outage. A 3-6 day outage for a top 3 cloud provider was shown to potentially result in total estimated losses of $6.9bn - $14.7bn with only $1.5bn - $2.8bn in insured losses.

The use of cloud computing services has proliferated to become the dominant mode of operation in 2018, with only 43% of global companies forecast to use traditionally built IT infrastructure on premises. In the race for fast adoption and shedding of in-house complexity, infrastructure-as-a-service provides faster deployment access to state-of-the-art infrastructure, greater scalability, higher security and availability than in-house operations, and CapEx shifted to OpEx, supporting faster growth and efficiency. However, the shift to cloud concentrates the organisation's information in the hands of a few 'hyperscale' suppliers e.g. Amazon (AWS), Microsoft (Azure) and Google. In 2018 an estimated 80% of large enterprises with off-premise workloads will hand off at least one workload to a hyperscale provider, although none have been immune from major outages.

On 19 April 2018, UK bank TSB announced that it would be upgrading its online systems that weekend. The company warned customers that some online banking services would not be available during the upgrade period. On the evening of 22 April, complaints poured in on social media. The majority of customers claimed they either received an error message when logging into the service or were denied access. Unfortunately, the migration changes that TSB had planned to implement to its online services turned out to be far more complex than a simple upgrade. By 2 May, TSB had been inundated by 40,000 complaints. Grilled by MPs at a hearing that same day, TSB's Chairman, CEO and COO were forced to admit that they could not guarantee a date by which this could be fixed[4]. While the closure of many lo-

#UberDown

"If you want to spot who is an #Uber driver right now, it's the car parked on the side of the road without blinkers on. #UberDown[8]"

@cwakelin on Twitter
July 1, 2016

- Resilience needs to be discussed within leadership teams not treated as an IT or risk register issue.
- Organisational leadership must encourage and empower senior individuals to critically discuss existential threats.
- The potential impacts of irresilience should be communicated early to boards so that mitigation can be incorporated into directional strategy.

cal bank branches had eliminated a human interface. Call centre staff accessing the same failed system were equally unable to provide any assistance. A "reversionary mode" was simply impossible. Chen Siqing, chair of the Bank of China has warned that the next financial crisis would arise as a result of online finance[5].

Even governments have acknowledged their abandonment of the ability to revert to pre-digital systems, or previous versions of the same technology. In evidence to the UK Commons Select Committee on Defence in December 2012, General Shaw, Assistant Chief of Defence Staff, was forced to admit that the UK had moved beyond "reversionary modes" if required to operate in a compromised cyber environment[6].

Risk and Opportunity in Equal Measure

Uber illustrates a fully digitally dependent business model. Its technology delivers profitability by efficiently matching supply and demand in a way not previously possible. Equally the company's digital resilience vulnerabilities relate to its own platform. On occasions when the system is inoperable, the business simply comes to a halt.

In contrast, traditional London black taxis are under threat from the redundancy posed by GPS satellite navigation technology, which calls into question the value of their specialist training (the "Knowledge"). These taxis, which are allowed by law to pick up passengers ad hoc, have drivers with no reliance on GPS technology and who can accept cash payment. While highly resilient to technology failure, the key question is whether the cost of that resilience can be passed on to the consumer. The Knowledge requires years of study that, in normal use, is fully replicated by satellite navigation. Given the near 100% uptime of GPS services and rapid improvement of crowd-sourced traffic applications, this business model currently relies on protective regulation to monetise knowledge that is largely redundant.

In recent months, a slew of closures and bankruptcies have dogged the world of retail. Retailer Toys 'R' Us failed to respond fast enough to the emerging threat of online retail platforms with the result that retail locations, which were once a benefit, became a handicap. The toy chain's administrators thought it "unlikely" that the retailer could be saved because its business model "isn't what consumers really want now". The majority of large businesses produce strategies with a 3-5 year outlook, too short a time period over which to completely re-engineer a business model and the requisite organisational competencies. In the context of a fast-evolving digital landscape, boards need be prepared to make major changes to adapt to new threats outside of the traditional analytic window.

Resilience in a Digital Context

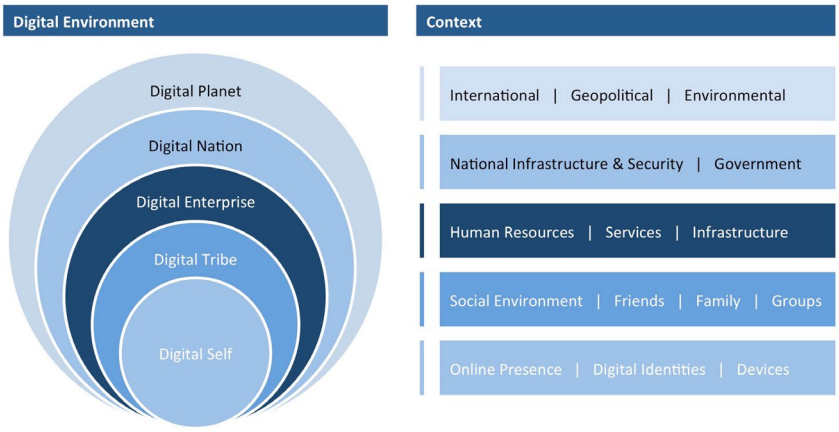
A New Model of Digital Context

The notion of a well-defined, defensible organisational perimeter needs to be replaced with a holistic approach to digital resilience that encompasses the complex multi-dimensional graph of interactions between employees, contractors, suppliers, partners, customers and digital services, all of whom share qualities of being both inside and outside. This multi-modal and multi-level supply of human and digital resources generates corresponding complexity around the identity, permissions and access control of individuals and devices. Organisations furthermore exist within the context of a national and global digital environment (Fig 2). Defences against a threat, perceived to be external, may become a source of irresilience once breached or if the threat comes from within.

FIGURE 2

A New Relationship with Risk

The "5D" Model illustrating the inner and outer digital environments within which organisations must base the context of their operational resilience.



Digital Self

Those entering the workforce today will be unable to remember a pre-internet world or a distinction between technology for work and for life outside work. The "Digital Self" refers to all of the "individuals" that contribute to an enterprise, whether human or machine intelligence driven agents, and their many technology components, interfaces and online personas.

Digital Tribe

Digital tribes form and reform globally at speed based on common interests. Customer advocacy through social media has immense power and traditional organisations struggle to manage the effects of fast moving campaigns as issues create influential tribes. If the digital tribe of a key human resource generates a stronger motivational force than a sense of belonging to the enterprise, trusted human resources may become a threat.

Digital Enterprise

In the pre-digital era, with clear demarcation of dependencies, risk analysis sought to identify individual risks and mitigate them. Critical resources and processes were kept 'in house', with outsourcing confined to non-critical and support functions.

Organisations possessed the internal capacity to improvise and recover to the previous state and could insure for those few remaining substantial risks.

Increasingly however, organisations are no longer defined by their physical presence and assets, but by the people, services and infrastructure that they comprise. Social media management platform Buffer has no headquarters, all employees work remotely and their salaries posted online.

The digital organisation now takes on the additional risks of their digital services suppliers. This tight coupling of processes and networking limits the usefulness of traditional risk models to mitigate or insure atomised risks accorded to the weighting of their probability and impact. Seemingly low impact hidden risks may generate high impact scenarios when coupled together.

"The volume of public cloud utilization is growing rapidly, so that inevitably leads to a greater body of sensitive stuff that is potentially at risk... We are in a cloud security transition period in which focus is shifting from the provider to the customer. Enterprises are learning that huge amounts of time spent trying to figure out if any particular cloud service provider is 'secure' or not has virtually no payback.[11]"

Jay Heiser
Vice President
& Cloud Security Lead
Gartner, Inc.

Digital Nation

The enterprise is critically dependent upon the resilience of national digital infrastructure and legal and regulatory environment, of the State(s) within which it operates and serves customers. Weak infrastructure, intellectual property laws and national requirements for data hosting and data privacy may generate vulnerability of the organisation to cybercrime, litigation (GDPR) or even state-level espionage.

Digital Planet

Technology adoption has the potential to impact global resilience, posing insidious and unforeseen systemic threats in the form of resource depletion, pollution and unsustainable anthropogenic climate change.

Blockchain technologies promise to transform transactional services with effective cryptographic security and resistance to many forms of cyber attack. However, whereas immutable distributed ledgers have been shown to ensure security and trust under normal operating conditions, they may undermine resilience in certain circumstances, through vulnerability to simple denial of service and timing attacks of the network being used to compute new transactions.

According to Digiconomist, the power usage of the entire Bitcoin network for the year 2018 is estimated to exceed 42TWh, or about 0.2% of global consumption, equivalent to 20MT of CO_2 emissions[9]. Credit Suisse further estimates that a price of $50,000, would be a Bitcoin mining incentive to raise electricity consumption tenfold, and at $1.1m, a sufficient incentive to consume the entire world's electricity supply[10]. Conversely a sustained drop in the value of that currency or an increase in energy costs will shrink that incentive. Slowing transaction times and restriction on the ability of users to trade may lead to a positive feedback loop, with participants unable to exit their holdings in the currency in the event of a "run".

"An organisational crisis is a high impact event that threatens the viability of the organisation and is characterized by ambiguity of cause, effect and means of resolution, as well as by a belief that decisions must be made swiftly.[12]"

Pearson and Clair (1998)

Assessing Your Digital Resilience Exposure

- Assess the ways by which digital irresilience may impact business model, processes, people and technology
- Assess capacity to innovate
- Build scenarios and worked through potential consequences.
- Map interactions of vulnerabilities, not isolated, atomised risks

Digital Resilience Assessment

Rather than address issues piecemeal, CEOs and their boards need to take a direct interest in digital resilience and adopt a strategic approach that embeds a resilient approach and culture within their organisations. Implemented strategies and solutions must be engineered in the knowledge that the challenges and opportunities arising from digital resilience will change constantly. It is intuitive to correlate security with resilience. However, while a less secure technology solution may pose vulnerabilities, a more secure solution may introduce flawed assumptions, irresilient processes or lead to catastrophic business inflexibility.

Organisations need to consider each technological decision not just in immediate cost/benefit but in terms of the capability/vulnerability paradox presented by resilience opportunity and irresilience risk. The costs, both in time and effort, need to be set against the potential costs of technology failure. Considering resilience requirements, it may be more effective to ignore reversionary modes and mitigate those risks through insurance or investing in crisis management capability.

Resilience is also a sensitive organisational issue, since points of irresilience are vital pieces of intelligence for competitors, and may run contrary to the corporate narrative that the organisation wishes to promote about itself. How these issues play out will determine the future power and prosperity of the organisation - and the careers of those leading it. To do this requires a mindset of being prepared to discuss and consider the issues with candour. The objectives of a digital resilience assessment are to consider what the leadership of the organisation should actually do, the digital resilience it should create, and the decisions it should make and prepare for.

Assess Organisational Goals and Priorities

The first step in assessment is to understand via executive interviews at a senior management level, by asking the following questions:

- What are the key goals and drivers, inputs and outputs of the organisation?
- How does technology drive the business model and organisation?
- Does the organisation have a documented and regularly updated operating model?
- Are business processes, systems and networks mapped and are the relationships between these understood?
- What are the major challenges facing the organisation in the short/medium/long term?
- Who has responsibility for digital resilience and what pro-

Institute for Strategy Resilience & Security
University College London

Shearwater Group

cesses exist in the case of a major resilience issue?

- What are the strategic and organisational processes for considering long term resilience of the organisation?
- What external technology dependencies exist?
- What resilience capabilities and competencies are in place?
- Who has responsibility for the long term business model and how is that aligned to technology development?
- Who has responsibility for the supply/maintenance of individual key systems and networks?

"Sooner or later something will go wrong, and we're very poorly placed to respond when it does. But I can't tell you what that something will be, or when it will happen.[13]"

Professor Paul Krugman

Nobel Memorial Prize Winner in Economic Sciences, 2008

"While remotely improbable events will happen rarely, there are improbable things that are guaranteed to happen every day. So you have to prepare yourself for things that have never happened before in the history of the world.[14]"

Lloyd Blankfein

CEO, Goldman Sachs, 2017

Describe the Current Operating Model

An operating model needs to describe the state of the system in its broadest possible terms; to identify the current operating model of the organisation, its organisational goals, processes, people, technology components, externalities and forces acting on the operation. These can be mapped out with iterative sessions to ensure consensus across the organisation that the model is capturing key issues of the digital environment and disruptive technologies that may be relevant to the organisation.

Building a Dynamic Resilience Model

Once a high-level operating model is agreed, this needs to be developed into a dynamic model that captures how the organisation and its dependent systems will change in response to changing assumptions, what the resilience issues are and what potential crises could arise. Having understood what changes or innovations could in theory be made, the organisation's capacity to innovate and implemente needs to be assessed.

Appropriate Levels of Digital Resilience

Taking risk is an integral part of doing business. There should be an appropriate level that an organisation is prepared to accept in pursuit of its objectives, which balances potential benefits and threats, depending upon the business goals and the nature of the organisation. Risk is often described as having only negative consequences and opportunity as upside. However, taking an opportunity, or not, also generates different types and levels of risk, the effects of which can be negative and/or positive. In safety critical areas, the avoidance of risk is paramount, while for an innovative project it may be essential to take risk to achieve success. Equally, resilience levels need to be appropriate to the objectives, growth stage and industry sector of an organisation. This concept is important in defining what resilience looks like on a case-by-case basis, and understanding that the objective of maximising resilience is not the converse of minimising risk.

- Appropriate levels of digital resilience will vary according to industry sector, organisational objectives and stage, as well as across the organisation.
- Boards and CEOs need to discuss and agree the level of organisational risk and irresilience that they are willing to accept.

Establishing An Active Digital Resilience Programme

- Actively build resilience for business processes, existing digital infrastructure and new infrastructure
- Put in place processes to encourage adaptive behaviour, continual evolution and learning environment

Building Organisational Capability

The EU General Data Protection Regulation (GDPR) is the most significant change in data privacy in two decades. Potential fines for non-compliance of up to €20 million or 4% of group world-wide turnover should place GDPR firmly on any board's agenda. Yet, considering the legislation was announced in April 2016, most companies seemed inadequately prepared. IBM reported that 70% of organisations were dumping data in the run up to GDPR's introduction in May 2018[15].

In a survey of crisis management professionals, 45% of CEOs were not involved in crisis planning exercises in those organisations that held them and only 30% of crisis management professionals thought their company would be able to handle an organisational crisis well[16]. Confidence in ability came from crisis preparedness capability, while obstacles identified were *senior management commitment* and the *effectiveness of decision making and team leadership*.

The roots of the failure to build digital resilience capabilities, lie not in technology but in organisational culture. Stronger direction is required to avoid compartmentalisation of issues within departments and elevate ownership to a leadership level. CEOs and their boards need to build resilience-by-design (Fig 3) capabilities both for themselves and their organisation at the appropriate level, including:

- **Resilience thinking:** ensuring the entire organisation incorporates resilience thinking about threats and opportunities.
- **Risk-based thinking:** understanding that effects of risk can be both negative and positive, and that taking or ignoring opportunities presents different types and levels of risk.
- **Cross-functional working:** discovering, creating and understanding new opportunities and threats requires cross functional working and a multidisciplinary approach.
- **Adaptability and flexibility:** ensuring the organisational culture and capabilities to enable decisions to be made and implemented within resilience-relevant timeframes and thereafter adapted as required in response to resilience threats.
- **Encouraging and empowering senior individuals to critically discuss existential threats**, with appropriate management mechanisms to collect and analyse these in combination.
- **A culture where the potential impacts of irresilience are communicated early** to boards so that mitigation can be incorporated into directional strategy.
- **Assessment exercises** that test the ability of the organisation and its management to respond, and highlight where decision-taking and capability gaps exist.

	Checkpoints for Resilience		Threats		Opportunity	
	Category	**Resilience Issues**	**Potential Crises**	**Traditional Risk Approach**	**Opportunities for Improvement**	**Resilient Approach**
Internal	**Digital Infrastructure Management**	Ability of organisation and external suppliers to ensure continuity of systems availability and a lack of reversionary modes	• Systems become unsupported • Problems in upgrading • Unable to recover systems	• Map systems and networks • Vendor assessment • Contractual agreements • Upgrade policy e.g. Upgrade to last but one version	• Reduce digital complexity and failure points • Eliminate legacy systems and costs • Switch to new rather than recover where advantageous	• Create IT roadmap • Map core processes • Map systems and networks • Identify vendor vulnerabilities • Contingency plans to accelerate change vs recovery
	Cloud Technology	Organisation becomes networked into the supply chain issues and vulnerabilities of the system provider	• Issues in supply chain of cloud providers are not transparent • Cloud outages	• Business continuity, contingency and disaster recovery processes • Contractual agreements • Vendor assessment	• Use of cloud technology offers better availability reliability and security over in-house systems • Plan for crisis	• Identify core process and cash flow vulnerabilities • Develop digital workarounds and alternative for core processes
	Information Storage and Recovery	An organisation is increasingly dependent on its data and code in order to survive	• Data is unable to be recovered in the event of a major outage	• Disaster recovery process • Business continuity planning • Crisis planning	• Ensure data can be recovered even with loss of system • Structure data to migrate onto alternative system for core processes in event of extended outage	• Simplify data as far as possible • Ensure separation between systems and data for core processes • Evaluate alternative highly scalable platforms
	Insider Threat	Deliberate misuse or lack of security awareness of individuals exposes organisation to malevolent attack	• Fraud • Ransomware • Cyber attack / terrorism • Staff use unauthorised work around systems	• Risk assessment • Compliance training • Periodic permission reviews	• Develop organizational competencies and values around customer privacy and security	• Risk mitigation maturity matrix • Map responsibilities • Consider permission resilience issues • Crisis testing
	Communications	Ability of organisation to survive from loss of communications e.g. Corporate telecommunications provider	• Degraded organizational capability • Isolated employees and poor decision making in crisis	• Contractual service agreements	• Respond more quickly than competitors. • Prioritise key decision making personnel and processes • Concentrate on what needs to be done to maintain cash flow	• Identify key personnel and core decision making processes • Determine order for recovery • Develop alternative communication tools for differing scenarios
	Networking Within Digital Infrastructure	Platform technology, internet of things , and APIs	• These technologies improve capability and ease of use but can introduce vulnerabilities	• Antivirus software	• Take advantage of network capabilities but prevent/ limit contagion by intelligent design	• Map core systems and processes • Design to create smaller isolated networks wherever possible
	Trustable Software	Auditability of the purpose, status and provenance of all software used by the organisation	• Susceptibility to software failure or cyber attack (both by insiders and external agents)	• Contractual liability • Vendor assessment • Employee vetting	• Certify products and services as trustable • Establish leading position in marketplace for trust and reliability	• Develop criteria and process for trustable software • Agreed audit methodology for releases
	Machine Learning	Use of algorithms are being used to make increasingly complex decisions but can reinforce bias in decision making e.g. Ethnicity bias	• Unprofitable decision making • PR and ethical problems due to bias affecting minority groups	• Encourage diversity in coding team makeup • Spot sampling and analysis of decisions	• Make more consistent decisions • Transparency in policy and decision making processes available to regulator • Position in market place as trusted company	• Code versions available for regulatory inspection • Publication of criteria used
External	**Cybersecurity and Terrorism**	Attack on digital infrastructure by outside forces	• Fraud • Ransomware • Loss of core systems affecting cash flow • GDPR breach	• Cyber war rooms • Monitoring systems	• Create resilience culture within team • Reassess threat in line with business activity and profile • Minimise attack surface	• Assess triggers and potential scale of threat to location, company and industry based on activity • Create a life long learning organisation
	Political/ Economic/ Societal / Technological	Long term trends and conditions that impact the business model	• Profitability • Existential threat	• Annual strategy review	• Re-engineer the company to adapt to new technology • Avoid existential threats	• Assess effects outside the analytical window of strategy processes • Be prepared to 'destroy' the company to 'save' it
	Location	Specific conditions (non catastrophic) affecting the principal business conditions	• Productivity issues e.g. Transport problems • Business continuity in event of major incident	• Ad hoc solutions • Business continuity planning	• Change organisational model and processes to maximise advantages and minimize disadvantages	• Determine issues • Develop measurements and review processes • Utilise technology to work around or eliminate issues
	Natural Disaster & Climate Change	Catastrophic event e.g. An earthquake in silicon valley	• Scarcity of essential resources e.g. Running water and communication outages disruption in short term • Business continuity issues in medium to long term	• Insurance • Disaster recovery process • Business continuity planning • Crisis planning	• Plan for certainty of event • Take advantage of lower asset prices in safer locations vs. Later	• Map core processes and assets • Redesign organisation • Relocate and protect core operational processes and assets

FIGURE 3

Examples of resilience-by-design approaches mapped across resilience checkpoints of an organisation.

References

1 Programmable Web API Directories : Programmeable Web 2017 https://www.programmableweb.com/news/programmableweb-api-directory-eclipses-17000-api-economy-continues-surge/research/2017/03/13

2 IOT Devices: Gartner Newsroom 2017 http://www.gartner.com/newsroom/id/3598917

3 Cloud Down - Lloyds of London / Air Worldwide https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down?utm_source=Presentation_screens&utm_medium=Presentation_screens&utm_campaign=emergingrisks_clouddown

4 Timeline of trouble: how the TSB IT meltdown unfolded https://www.theguardian.com/business/2018/jun/06/timeline-of-trouble-how-the-tsb-it-meltdown-unfolded

5 China Banking News: http://www.chinabankingnews.com/2018/06/14/online-finance-will-trigger-next-financial-crisis-bank-china-chief/

6 UK Commons Select Committee December 2012 https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm

7 Figure 1: IOT Devices: Gartner Newsroom 2017 http://www.gartner.com/newsroom/id/3598917; Programmable Web API Directories : Programmeable Web 2017 https://www.programmableweb.com/news/programmableweb-api-directory-eclipses-17000-api-economy-continues-surge/research/2017/03/13; Artificial Intelligence Revenue: Tractica https://www.tractica.com/newsroom/press-releases/artificial-intelligence-revenue-to-reach-36-8-billion-worldwide-by-2025/; Data Centre Investment: Data Centre Realty http://www.datacentrerealty.com/blog/; Artificial Intelligence Revenue: Tractica https://www.tractica.com/newsroom/press-releases/artificial-intelligence-revenue-to-reach-36-8-billion-worldwide-by-2025/ Mobile Device Users: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/ Global Cyber Security Spend http://www.exciteit.com.au/blog/future-outlook-cyber-security/ , Augmented Virtual Reality Spend http://www.theinsightpartners.com/reports/augmented-reality-and-virtual-reality-market, Big Data Market Size https://www.statista.com/statistics/254266/global-big-data-market-forecast/

8 Yes, Uber is down so you'll need to find another way home https://www.fastcompany.com/4012625/yes-uber-is-down-so-youll-need-to-find-another-way-home

9 Digiconomist: https://digiconomist.net/bitcoin-energy-consumption

10 Bitcoin's energy usage is huge – we can't afford to ignore it https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

11 Jay Heiser, Gartner https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

12 Pearson & Clair 1998 http://issueoutcomes.publishpath.com/Websites/issueoutcomes/Images/Reshaping%20crisis%20management%200DJ.pdf

13 Can the Economy keep calm and carry on, Paul Krugman https://www.nytimes.com/2018/01/01/opinion/can-the-economy-keep-calm-and-carry-on.html?_r=0

14 Lloyd Blankfein interview with Jeff Cunningham https://medium.com/iconicvoices/goldman-sachs-ceo-lloyd-blankfein-e5247d46b25e

15 Preparation for GDPR https://internetofbusiness.com/ibm-study-gdpr-opportunity/

16 Crisis Management Insight Survey https://regesterlarkin.com/news/crisis-management-insights-survey/

Digital Resilience