Everything you need to know about Data Protection and AI

This is a summary transcript of a talk given by Emma Martins to The NED Forum on 24 July 2023.

"*…if the rate of change on the outside exceeds the rate of change on the inside, the end is near.*" - Jack Welsh, former Chairman and CEO of General Electric

We need to acknowledge is the extraordinary pace of change that we are experiencing across all areas of our lives, particularly in technology and data.

The 1992 Cadbury Report talks of the role of the Non-Executive Director (NED) as bringing *".. independent judgement to bear on issues of strategy, performance and resources.*"

That means that the role needs to centre around governance, accountability, strategy. Not only where the organisation is going, but why it's going there and how it intends to get there.

NEDs need to be a 'critical friend' and need -

- The **will** to challenge
- The **skill** to challenge
- The **knowledge** to challenge

Lots of things NEDs deal with are increasingly complex – including data and technology. Technically, what sits behind intuitive, effective systems is a wealth of technologically advanced processing and large data sets. That doesn't that mean board members simply have to leave it all to the experts (either inhouse or outsourced).

You obviously can't be over every aspect of your organisation, and indeed that's not your role, but you are faced with having to prioritise – so you need to work out how to do that effectively – how to focus on important/high risk areas.

Data is at the heart of most organisations, regardless of size or sector. And data is now a business performance issue, not just an IT one.

We should all think about our own organisations – what do the inputs, processes, outputs look like in the context of data and technology?

So, if data is a business performance issue, we need to recognise that it gets to the core of operational resilience which is, by definition, a priority for all of us.
Operational resilience is not a separate issue to data protection or cyber security – it is intrinsic to it. It follows, therefore, that defence against cyber/data breaches is utterly dependent upon operational resilience.

Every day we see stories of cyber attacks, cyber threats. We need to take care not to become desensitised to these because they are so common – because we are all vulnerable, each and every one of us and the organisations we work for.

But language matters, a lot.

Take a moment to think about what cyber actually is?

'Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool — and therefore strange, spooky.' [New York magazine, Dec. 23, 1996]

Here is a reasonably sensible definition of it –

'relating to or characteristic of the culture of computers, information technology and virtual reality'

Is there anything that any of our organisations do that doesn't in some way involve these things?

So, we should agree not to think of it as strange or spooky, but simply part of our everyday business activities and of course personal activities too because so much of our lives is digital these days.

Some examples of operational resilience risks –

- Outsourcing/3rd parties
- Bring your own device ('BYOD')
- Update/patching requirements
- Changing backdrop of data privacy
- Cloud computing
- Legacy systems
- Regulatory environment
- Globalisation and professionalisation of cyber crime
- State sponsored attacks
- Insider threats

Outsourcing can be an example of where we can ask good questions.

More of us are reliant upon cloud services and there are absolutely advantages, for example

- Reduced running costs

- Reduced future costs
- Network protection
- Processing power/storage

But, whilst the data of our organisations may sit somewhere else, and with someone else, you are still very much responsible and liable.

Few of us would call ourselves cloud experts but does that mean we can't be part of the conversation? If our organisation has liability, that's one very important reason to answer that NO – of course it doesn't mean we can't be part of the conversation. In fact, we can't afford **not** to be part of the conversation because it gets to the heart of our businesses, our governance, our risk, our success, our failure, our very existence as a business.

Here are some examples of things we can all ask -

- **Where** is our provider based?
- What **contract** do we have in place with them?
- **Who** is responsible for that contract?
- Do we conduct any **audits**?
- How easy would it be to **change** provider?
- What is the process for **reporting** data/cyber issues?
- **Who** gets notified (our end)?
- **What** do they do with that notification information?
- What is our **comms** plan?

Look at how simple these questions are? None of them require us to have a degree in computer science but these are some of the most important questions that need to be asked. They require us to understand the context of these things against the backdrop of our organisations, and they require us to understand our own roles and responsibilities.

And these questions are relevant for anything outsourced, cloud is just one example.

So we don't need to be experts – remember this:

"…it is critical to remember that what we are holding to account is not machines themselves, but the people who build, own or operate them – including any who alter their operation through an assault on their cyber security. What we need to govern is the human application of technology: what we need to oversee are human processes of development, testing, operation, and monitoring." - Professor Joanna Bryson.

And whether or not any operations or activities are outsourced, data governance /security/cyber should be top of mind for every NED, regardless of sector. And we need to have the will, skill and knowledge to ask those key questions.

One area that comes up a lot, and you may see that we do regular public updates on stats, is data breaches.

Again, we can ask some key questions -

- **how** have we assessed our risks?
- **who** is involved in assessing those risks?
- how are we **responding** to those risks?
- **who** is responding to those risks?
- what can we all do to **reduce** the chances of bad things happening?
- **when** something bad happens, **how** do we respond and how do we recover?
- **how often** are we, the board, talking about these things?

And these are absolutely front and centre operational, governance, resilience issues, not just technological ones.

NEDs must ensure that their executives are doing what they need to be doing – that they have thought through and practiced, that they understand the reality of the risks rather than cutting and pasting a policy that never sees the light of day.

Getting that embedded into business as usual is a **cultural shift**.

That sounds so simple but time and time again we see culture being at the heart of failures, of mistakes, of incompetence and of bad outcomes.

You can have all the shiny policies, procedures, vision statements you want, but it's only the *actual behaviour* that counts.

"*Culture forms and develops as people throughout the firm judge management on managements judgements.*"

And of course culture is way beyond ticking of boxes. It is active not passive and it can be a huge force for good, as well as a huge force for bad.
Neither is luck.

That's where we need AI.

We have heard so much about it in recent months and rightly so. It is changing everything and will continue to do so with increasing speed, breadth and depth.

More than anything we need **human** skills and we need to ask questions that matter. If anything, these questions are more critical than ever, and the absence of them more problematic and even dangerous.

So, I want to argue that all you need to know about AI, is that it needs to refer to *anthropomorphic intelligence*.

For boards, that's individuals bringing experience, wisdom, knowledge, perspective, emotional intelligence, humility – lots of things that AI cannot deliver. Not only the 'what' we do but the 'why' and the 'how' we do it.

Some things to think about putting on a to-do list –

- Have data/cyber as a standing item on your execs meetings agendas and your own board agendas. It should be on the risk register. Have a discussion with your teams about the word *cyber* – ensure it's not putting people off engaging. Find language that works for you and that includes everyone and is relevant and meaningful for you and your organisation.

- Find out when your organisation last had an exercise to run through its response to a catastrophic data breach. What. When. How. Who. The details matter, and so do the learnings.

- Work to stop treating weaknesses in information security as a purely technology problem. It's as much (if not more) a *people* problem. And if it's a people problem, there is a people solution.

- Know that awareness isn't enough. You need to **influence** behaviour.

If you are non-technical – good. You absolutely need technicians. But you also need diversity – of thought, experience, approach. And that's where boards come in. That's where good NEDs come in.

What are some of the common problems?

- I think we are prone to look at technology and say 'what can it do' when what we should be asking is 'what do <u>we want it</u> to be doing' / 'what <u>should</u> it be doing'. It doesn't have a life of its own.
  Sometimes we think the trajectory is set. It's not. <u>We</u> set it.

- Applying inadequate skills to the issue.

- A lack of board understanding of these issues, their place in conversations, in strategy, in operational considerations and in risk.

- Insufficient organisational support for data protection/security.

- A failure to appreciate how wrapped up these issues are in customer/client confidence and trust.

- Treating compliance and operational resilience as a tick-box exercise.

- Underwhelming and ineffective communication/support/awareness/training.

- And last but very much not least, again - the human factor. It is a lot more important than most of us think. There needs to be mindset change.

When looking at risk management we need to understand people. People will always make mistakes. We will always make mistakes.

But probability can be reduced.

And impact can be minimised.

Risk management is so much about people management.

When something goes wrong it can be damaging for your organisation, but we must never forget that behind data sets are real people. And there are lots of organisations that have your data, and the data of your family and loved ones – I care about what happens to that, and I am sure you do too.

It's not enough to go away *thinking* about this, I want you to go away *doing* it. Awareness isn't enough, it's behaviour that matters, it's behaviour that impacts outcomes.

Here are some data related questions you can consider asking –

- What personal data (about people) do we have?
- Who is the data protection officer/lead? (*Have a chat and a cuppa with them*)
- What does our breach response look like?
- Have we run a tabletop exercise?
- How could we understand data/cyber risks better?

- Is it on the board's radar?
- It is on the board's risk register?
- (There are lots more!)

What you need to know about data protection, is that it's an issue for you, your organisation and for everyone in it.

What you need to know about AI is that I want us to look at it as 'anthropomorphic intelligence' – your intelligence that's needed perhaps more than it's ever been needed.

I want to take this opportunity to thank the NED Forum, particularly Tina and Gordon, for giving me a platform to talk about this over the years. It's been a huge pleasure and as I near the end of my fixed term, I want to express my gratitude. I hope some of what I have been able to say has been useful to some of you.

I believe very strongly that data, done well, can differentiate an organisation and indeed jurisdictions. Lots of risks with this stuff, but equally lots of opportunities – if we decide to take them.

Related resources:

- Guidance on using AI systems with personal data.
- Your organisation's legal obligations under data protection law.
- Resources for shifting culture: Project Bijou.