Reviews and miscellaneous

Throughout 2020 we attended a variety of (mainly) online conferences, exhibitions, seminars and read books many of which we reviewed for our blog. Also other subjects caught our interest and these are included in this collection.

IoT and Industry 4.0 Online Conference 16th June 2020

Image by Pete Linforth from Pixabay

Dickson Ross, the Editor-in-Chief of Engineering and Technology magazine, introduced the conference

He pointed out that although IoT is real and growing rapidly, it can be difficult to explain the benefits to people. Many of the standard applications in the home can be underwhelming. Industrial applications too may be unexciting, but at least these can be genuinely profitable. Monitoring and predictive maintenance for example can reduce costs of failure and by scheduling maintenance effectively reduce off-line time for industrial processes. The first talk addressed these sorts of applications.

Martin Walder, Schneider Electric – Practical steps to your Ind 4.0 factory

Industry 4.0 is represented by automation, robotics, and IoT sensors, so many people think it is only applicable to Blue Chip companies. In fact, by taking a staged approach it can be for smaller companies too. Schneider Electric advocate a "Tailored, Sustainable, Connected" approach and have demonstrated 5-15% cost savings and reduced energy consumption in their smart factories, some of which are designated by the WEF as "lighthouse" factories, showing the way to others.
They divide the systems into 6 areas:

-
- Agile Management – all digital, data collected;
- Process Efficiency;

- Asset Performance management;
- Empowered operators (providing them with data);
- Reliability;
- Energy efficiency

And for each of these there are three layers:

-
- Connected products (sensors);
- Edge control – smartphones or other devices;
- Apps

Example applications included:

-
- Using Machine Learning to provide predictive analysis based on IoT sensors for preventative maintenance without affecting production flow.
- Empowering operators with real-time data and supervisory support to reduce maintenance time
- Augmented reality to support seasonal workers whose training was cut to days from months

A critical point is that because everything is data-driven you need your cyber-security to be top-class. Smart factory is mainly about software, not expensive machines; as you upgrade equipment make it connected and share data.
Their philosophy is to “Think big, start small, scale fast”. Encourage bottom-up thinking to create incremental ideas, build these into pilots, and if successful then scale fast; if not, fail fast too. This works better than getting a top-down spec from senior management that never gets delivered.
Management should identify focus areas, and build methods of standardisation and roll-out discipline, comparing and sharing best practice rapidly. Everyone becomes engaged.

Anthony Shingleton, Simpler Consulting (IBM) – 10 reasons why your Industry 4.0 and IoT transformation might fail

Anthony approached the implementation of IoT and Ind 4.0 as one of transformation, rather than simply of technology. So his 10 points emphasised other aspects of the organisational and cultural setting that need to be addressed for a successful outcome.

1.

1. Organisation/Operations 4.0: will the operational people be able to work with the tools? Or will they be like cavemen with smartphones?
2. Culture 4.0: will the availability of detailed data be used by management as a way of helping staff, encouraging them to learn; or to blame them for not hitting targets?
3. Project Execution: in an era of rapid change there is a need to reduce project lifecycles; Gantt himself said that Gantt charts don't cope well with change.
4. Don't just address individual tech developments; focus on system thinking, the interaction of the parts
5. Organisational design: need to consider the FLOW of data, insight and knowledge around the organisation, and who is enabled to do what.
6. Start with goal, a cleartop-down vision; unlike Walder's recommendation of bottom-up leads, you should pick pilots that fit with the goal. Let people know where they are going, and so inspire them on the journey.
7. Set "Breakthrough Ambition" targets that make a real difference, rather than just incremental pockets of improvement. Set clear challenging targets and create confidence that these can be reached
8. Identify "Success Measures" that fit the company strategy; otherwise the focus will become just on the cost.
9. Need to get flows between all parts at the same time, the synergy between the pieces is what brings the real benefits
10. Don't simply digitise a wasteful system; simplify and clarify, take advantage of new things you can do.

Jason Lessard, HSF – Will Industry 4.0 kill your competitive advantage?

Industry 4.0 installations will expose your proprietary data and knowledge, and open up your secrets across the whole supply chain, to contractors and to disgruntled employees and ex-employees. Your information will be exposed, your USP visible, even to the extent that the supply chain could cut you out. Will your current information security strategy work in this environment?

The key points are:

-
- You will only thrive if you have competitive advantages; you must understand what they are and how vulnerable they are; conduct a risk assessment

- Make sure you know which is IP protected; identify how to use these to protect your competitive advantages.
- Take steps to protect IP through patents and make good use of unregistered rights such as copyright
- Trade Secrets are of commercial value, but you need to have taken steps to keep them secret from them to be recognised. Build a register, have an access control system, enforce confidentiality obligations.

Yasir Sheikh, Honeywell – Confluence of Tech trends; redefining what's possible with today's buildings

The development of IoT, Cloud and Big data is enabling the creation of "Smart Buildings".

The key megatrends that Yasir identified were:

-
- Embedded chips
- Connected everything
- Control by code
- AI

We can now move on beyond monitoring a building's health (status of systems) to predicting what will break down next, and even further to building self-healing systems with autonomous responses.

The problems that tend to remain are:

-
- Silo responsibilities;
- Enterprise complexity;
- Remaining areas of manual control that cannot react fast enough.

Reflections

The differing approaches of Walder and Shingleton (bottom-up, incremental vs goal-oriented, directed) were intriguing and probably reflect their faith in the power ot technology. Shingleton no doubt correctly places great weight on the organisational context of the tech transformation. This has always been the case, notably the point about automating ("computerising", we used to call it) ineffective systems rather then re-designing them.

Neither addresses the wider context within which the transformations are occurring, the economic and societal attitudes of the people in the system. For that, a wider scenario approach is required.

Nonetheless, it is clear that IoT and AI will bring radical changes to industrial organisation over coming decades, with many interesting second-order effects. One to keep on your radar.

Written by Huw Williams, SAMI Principal; published 1 July 2020

Cyber Risk - Should boards be concerned?

Image by mohamed Hassan from Pixabay

The short answer is 'yes'. Boards should be very concerned. Cyber risk is a growing threat for all organisations. If an organisation has not already suffered a cyber-attack it almost certainly will in the future, probably sooner than later.

I chair a group called the Control and Risk Self-assessment Forum. We meet from time to time to discuss risk and governance issues. In January we spent a day discussing cyber risk. The event proved highly popular with all the available places being taken within 24 hours of listing the meeting. We were kindly hosted in London by the Institute of Risk Management who also offered to publish a report of the discussions. This article is a short summary of what's in the report. The report itself, and details of the speakers, can be found here. Many of the participants had personally been affected by cyber-attack.

In the UK, many public sector National Health Service hospitals were hit by WannaCry ransomware cryptowormattacks in 2017. We heard from a former non-executive director of one hospital. The attacks, which targeted computers running Microsoft Windows, temporarily crippled activities. Almost everyone was affected and, amongst other things, surgical operations had to be cancelled. The hospitals were not specifically targeted but were vulnerable because they had not properly protected themselves; a key oversight was that software updates had not been installed. This should be a salutary lesson for any board thinking their organisation is not a target and so will not be attacked.

Many organisations are under prepared and few boards have the skill set to understand the risk fully. They may also not understand who below board level is or should be responsible for protecting the organisation against cyber risk. It may be that no one actually regards it as their responsibility. Security is not the first concern of programmers, chief information officers (CIOs) or chief technical officers (CTOs). Software developers are rarely security experts, they are paid to get a program operational and security may not feature in their thinking unless it is part of the brief. Until an attack happens CIOs will be more interested in operational matters along with CTOs who may prefer to spend money on new technology than on cyber security. Similarly at management and C-suite levels there are likely to be many competing priorities meaning that security concerns get trumped by operational or cost issues.

In our discussions there was a general view from both speakers and participants that most boards lack anyone who understands digital risks and few board members know enough to ask the right questions of their staff. For example do directors know exactly where their data is, might it in fact be in another country? The fact is that, as one of the speakers Sue Milton pointed out, technology is now a utility. But it is an increasingly complex one, where no one individual understands all the detail. This means the causes and effects of cyber risks are underestimated.

Another speaker, Dan Roberts, took us through some fascinating role-play where in one session we role played staff at management level and C suite level executives in another. In both it became very clear that cyber security issues are unlikely to get the attention they need because everyone else, apart perhaps from risk managers and internal auditors, will be more concerned with operational matters, project delivery, maximising revenue and keeping costs down. Addressing security concerns costs money and takes time so many people won't want to be bothered especially if other priorities are delayed. In our role play, no one was willing to delay operations to address security concerns. As a result, none of the teams agreed to deal with them. It is very easy to ignore a risk until it actually happens. Several of the participants reported having had similar experiences in real life.

Many organisations understandably have a culture of rewarding delivery – of getting things done. This is generally a good thing but not if it means that other important issues are not properly addressed. Such issues could include expressing concerns. CTOs and CIOs, like most managers, are unlikely to admit to failings or risks – unless they see this as a way of sharpening focus on their priorities or the ability to raise their budgets.

So what can be done? Perhaps the first and most important thing is to ensure that boards have sufficient buy-in to cyber security risk and genuinely own the issue. One possible approach is to make it clear that cyber risk could put the organisation out of

business – and directors could suffer personally. This may focus people's minds and enable proper resources to be applied.

Boards can be taken through a model of cyber risk with examples:

1. Threats: from various actors, criminals, states, disaffected insiders.
2. Vulnerabilities: unpatched systems, "bring your own device", poor training and awareness, poor supplier change control systems.
3. Exploits: phishing, Distributed Denial-Of-Service (DDOS), social engineering (i.e. getting people to talk about the security system).
4. Outcome: fraud, reputational damage, IP.

Every director on a board should know who in the organisation is responsible for addressing cyber risk and ensure the board, and relevant committees such as the audit committee, give at least as much attention to cyber risk as they do to other key risks. They also must ensure they know which questions to ask, where they can get answers and make sure they can understand and, if necessary, challenge the answers they get.

In our final session we brainstormed how managers could get their boards more engaged on cyber risks:

1. Create an awareness of the scope and scale of the threat; rate the organisation's, and the board's awareness of the threat.
2. Ensure good training within the organisation, and at board level, about the threat and its mitigation.
3. Build a roadmap for how the Chief Risk Officer (CRO) and others could persuade board members of the seriousness of cyber risk (ie it's not a one-off); CROs to lead.
4. Identify what information there is in the organisation and where and how it flows. Define information needs – who, why and how they will get it.
5. Identify and assess the at-cyber-risk assets and targets.
6. Explicitly define the cyber risk acceptance or tolerance level – and the "Crown Jewels" which need protection; set target risk as well as net risk and analyse the difference. Do this at a Board away day.
7. Use a 2×2 box grid of impact and likelihood as a starter methodology for the risk ignorant then carry out SWOT analysis.
8. Explore different scenarios of what might happen and how risk can be mitigated.

9. Recognise that at some time the organisation will be hit by a cyber attack and so build a response plan.

10. Consider if people properly understand the product or service business model and the risks to it and the associated information business model.

11. Boards are reliant on having the right people in the organisation supporting them. Review if the right people are in place; do they understand the processes?

12. Answer the Canadian CPA paper '20 questions on cyber security'.

Written by Paul Moxey, SAMI Fellow and Visiting Professor of Corporate Governance at London South Bank University and author of a textbook on corporate governance and risk management. He has chaired the CRSA (Culture, Control and Risk Self-assessment) Forum since 2000. He lectures widely and provides executive education and consulting support on governance, risk management, business ethics and culture. A former financial controller, company secretary and management consultant, from 2001 to early 2015 he was Head of Corporate Governance and Risk Management at ACCA where he was involved in governance developments across the world, including speaking at conferences and other events in five continents as well as a considerable amount of writing. His main work interest is in the behavioural aspects of governance and risk and his last major project at ACCA was to lead an ESRC funded international research study of corporate culture and behaviour.

Published 28 October 2020