What could move the dial?

Background

Sue Milton, Ed Steinmueller and Gill Ringland met to discuss:

The Working Group's aim is to improve Availability of services relying on IT systems. What messages are needed to do this & who needs to "get" them?

The first message is that failures of IT systems will happen, as emphasised by the UK Government to CEOs of FTSE "50 companies: they have written urging them to look beyond cyber-security controls toward a strategy known as "resilience engineering", which focuses on building systems that can anticipate, absorb, recover, and adapt, in the event of an attack."[1]

Second, we agreed that many organisations are making "sensible" choices[2] around IT – eg Amazon, Microsoft, Google, IBM, SAP, Oracle, Salesforce. Plus industry standard packages by sector. The reasons for choices include

- Scalability
- Expertise
- Support (SLAs)
- Forward path

However, all of these suppliers have complex supply chains with components from many sources, which may compromise resilience. SLAs may be a moving target and unenforceable. What can move the dial so that accountability for the availability of IT services is widely accepted and implemented in the public and private sectors?

Cyber

Boards and Governments are rightly concerned about cyber attacks. While not all IT failures are due to cyberattacks, many of the measures introduced to guard against/ameliorate the effects of cyberattacks will improve the resilience against

[1] https://www.bbc.com/news/articles/ced61xv967lo
[2] "Nobody ever got fired for choosing IBM"

other types of failure. These include approaches to system architecture, anticipation, and recovery[3].

What and who can change the dial?

Statements from the UK Government

The UK Government has started to change the dial with the current Cyber Security and Resilience Bill[4]. It applies to CNI[5] and OES[6] organisations, and is to be enforced by regulators using the NIS framework.

The regulatory regime was seen by us as questionably effective, but the climate setting from the Bill is useful.

In addition, the UK Government has issued a Cyber Action Plan [7] for the UK public sector which states:

Government-wide cyber risk will be owned by the DSIT Permanent Secretary as Government Technology Risk Owner.

And for Organisational cyber risk ownership

The Accounting Officer is the senior official (Permanent Secretary or CEO) with overall accountability for an organisation. This includes personal accountability for the cyber risk of that organisation.

For LGD[8]s, that accountability also extends to the ALB[9]s and sectors which fall under their financial responsibility. For all government organisations, it extends to appropriate assurance of the cyber security and resilience of their suppliers.

---

[3] https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/

[4] https://bills.parliament.uk/bills/4035

[5] Critical National Infrastructure

[6] Other essential services, eg including health

[7] https://assets.publishing.service.gov.uk/media/695c0c83295a95414df21b4c/E03515734_-_Government_Cyber_Action_Plan_ELAY.pdf

[8] Lead government department (LGD): A government department that has other public sector organisations within its purview. LGD is usually the department with primary policy responsibility for the risk and expertise for the area impacted by the emergency scenario.

[9] Arm's-length bodies (ALB): A commonly used term covering a wide range of public bodies, including non-ministerial departments, non-departmental public bodies, executive agencies and other bodies, such as public corporations.

Accountability in the private and NGO sectors

Regardless of business type the responsibilities of board members include[10]:

- establishing vision, mission and values
- setting strategy and structure
- delegating to management
- exercising accountability to shareholders and being responsible to relevant stakeholders.

Risk is flagged by the IoD:

Determine the company's appetite for risk and engage in the process of backing a robust risk management programme focused on the company's business and the area(s) of its activities.

However, Boards in the private sector are not yet aware of the liability and reputational risks of IT failures[11].

What can reset the dial with Boards to increase awareness and then resilience?

With what messages?

Responsibility to stakeholders includes legal compliance. This is necessary but not sufficient, and there is no generic legislation for availability of services, though some sectors, eg telecoms, do have published SLAs for services to customers, and published penalties.

Sue has used one question with Boards: what are the 5 nightmares keeping the Board awake at night? A frequent immediate response was "Bad headline in the Daily Mail/viral on Social Media", i.e the organization's public image and reputation. This related to a number of nightmares, of which a number were IT related

- Data corruption/loss
- Supply chain fiasco (including but not just software)
- Failure of a major strategy eg acquisition
- Disruption eg loss of site/people or Important Business Service

[10] https://www.iod.com/resources/company-structure/what-is-the-role-of-the-board

[11] https://cdn.sanity.io/files/33u1mixi/production/0503ea6e1f86300ba54319afe8db48bbe6632bae.pdf

What IT people need to do

They may need to consider configurations and poor operational planning and processes, across the organisation. This needs IT people to develop networks across the company, in the absence of a Site or Systems Reliability Engineer with responsibility for Availability.

They need to understand the three aspects of resilience engineering[12], and how they contribute to "anticipate, absorb, recover, and adapt" as in the FTSE 350 letter.[13]

- Architecture: the design principles for resilience in new systems can be used to adapt existing systems to meet the needs of new users and application, and to reduce failures due to attempted upgrades.
- Anticipation: key is monitoring, measurement and analysis, to support action to detect and avoid potential failures; to absorb and limit the scope of failures, and to provide information for recovery after failure.
- Recovery: integration with Business Continuity Planning, Incident Response and Disaster Recovery Plan; war gaming, training, reviews; Backups and supply chain management.

They need to apply them to each of the four nightmares above. Then they can set priorities, provide plans and costs for improvements under each heading.

So the messages for Boards are

- IT system failures will happen, not all due to cyber attacks.

- The organisation's public image and reputation faces risks from IT systems failures.

- Your IT people can quantify and recommend steps to protect your reputation.

[12] The ITLF Availability Working Group is pulling together a Handbook with Guidelines, Tools and Case Studies

[13] https://www.gov.uk/government/publications/ministerial-letter-on-cyber-security-to-leading-uk-companies/ministerial-letter-on-cyber-security