Availability: Improving Service Resilience

Summary

This document summarises the slides used at the online event on 30th June 2025.

This is a BCS event by Video Conference in collaboration with Business Continuity Institute (BCI).

Speakers: Alice Kaltenmark,
Global Technical Resilience (TR) Governance Lead, LexisNexis
Director on The BCI Global Board
President, Kaltenmark Consulting, LLC

Gill Ringland
Co-chair, Service Resilience Working Group
Co-author, Resilience of Services, reducing the impact of IT failures

Chair: Paul Reason

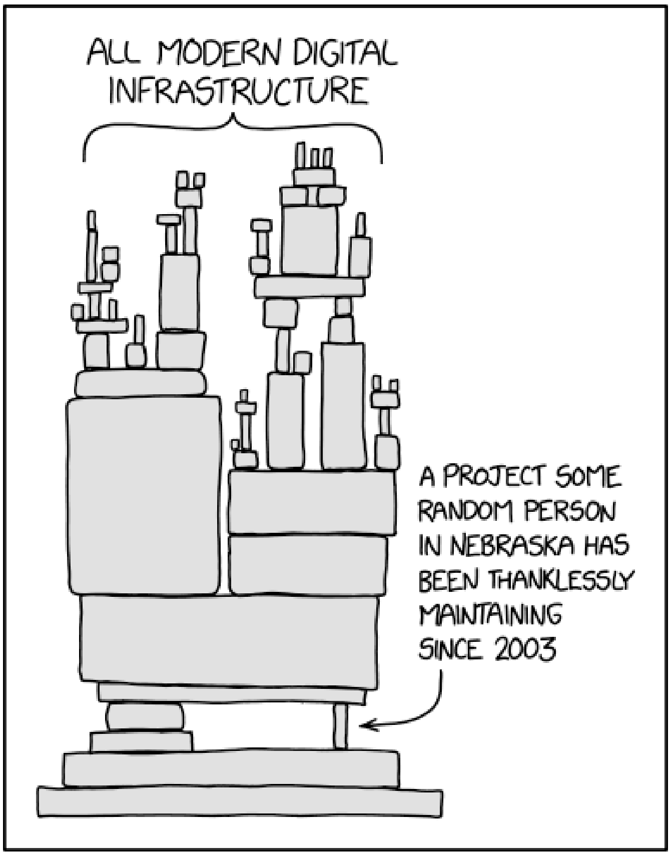
Summary of why we are here

- Digital services are expected to operate as a utility,
- But all systems can fail.

So the need for Business Continuity first.
As well as reducing frequency and impact of failures, improving resilience.

The Landscape:

Based on the work of BCS ITLF Service Resilience Working Group) the following diagram represents the state of the systems that are supporting our business.


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

- IT is now a utility – users expect 7/24 availability
- Software is inherently fallible: it fails
- Software has a long life, and most new software is not developed in house
- IT failures have significant impacts on GDP and productivity
- Cyber-attack is not the principal threat to resilience
- AI won’t fix resilience problems anytime soon

We address these issues in 2 parts

1. Business Continuity - How to recover the service!
2. Reducing frequency and impact of failures - Tools to improve resilience

Business Continuity

Resilience: ability to absorb and adapt in a changing environment

Resilience Basics

Data Protection – backups, snapshots, offline / off-account backups
Dependencies – what do you need to restore?
Plan – list of tasks to restore / recover
Test – does it work? Need proof!

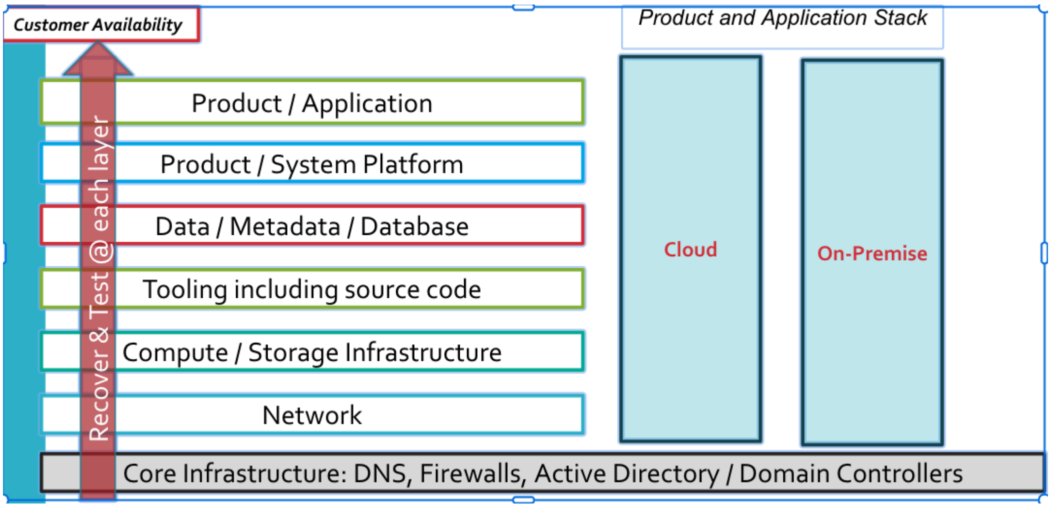
Resilience Threats

Failure – process, application, infrastructure, network

Corruption – data loss, data corruption, configuration corruption
Cyber attack – malware, ransomware, infrastructure encryption, data encryption

Restore & Recover Basics

Assuming our solution set is build of the following stack


Customer Availability
Product and Application Stack
Product / Application
Product / System Platform
Data / Metadata / Database
Tooling including source code
Compute / Storage Infrastructure
Network
Recover & Test @ each layer
Cloud
On-Premise
Core Infrastructure: DNS, Firewalls, Active Directory / Domain Controllers

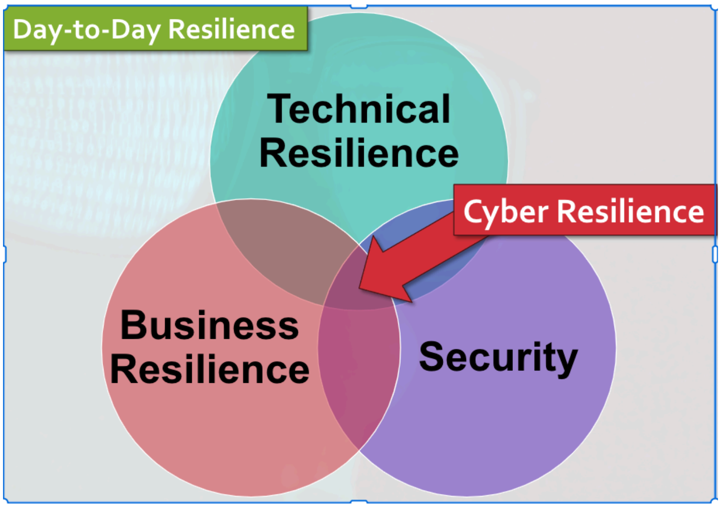
We will then apply the following basics to each layer of the stack:

- Data Protection: backups, snapshots, offline / off-account backups
- Dependencies: what do you need to restore and in what order?
- Plan Playbook: prioritized list of tasks to restore / recover & how long will it take?
- Test: does it work?

In all cases we need proof with documented & reported results

Cyber Resilience

A special case as it needs additional steps to ensure that there is no corruption.



- From scratch recovery required – building from 'bare metal'
- Immutable backups for data protection including:
  - Network – including configuration metadata and security controls
  - Servers – configuration metadata
  - Databases
  - Storage
  - Source Code
  - Deployment pipelines
  - Documentation – recommend storing with Source Code
  - Applications
  - Operational Tooling
- Testing vital to demonstrate capability

Resilience Perspectives by Owner

Product / Business Owner

Set the product / business resilience objectives – customer outage tolerance and data loss tolerance

- Business Impact Analysis helps to determine the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO)

Prioritize and fund the work needed by the teams to design and implement resilience for your product / system / application

Support regular testing of resilience capabilities

Developer

Design and implement the product / application to meet or exceed the requirements

- Comply with Engineering and Architecture guidance on data protection, security controls, and resilience documentation

Validate resilience capability using approved testing and deployment methodologies

- During initial development and iteratively with every sprint and deployment – continuous improvement
- Adhere to Engineering and Architecture guidance for effective testing methods

Report results of testing and documentation updates

- Working with Engineering for automated methods of reporting results and plan updates

DevOps Engineer

Design and implement the operations infrastructure and processes to meet or exceed the requirements

- Automation of compliance validation, resilience testing methods and reporting of results

Validate resilience capability using approved testing and deployment methodologies

- Routine testing of infrastructure resilience as part of daily operations

Collaborate with site reliability engineering, network, security, infrastructure and development teams

- Socialize best practices and help guide teams to comply with resilience principles and requirements
- Establish and maintain resilience best practices and requirements in partnership with Engineering and Architecture

Customer Expectations

- PRODUCTS ARE ALWAYS AVAILABLE – NO MATTER WHAT IS HAPPENING IN OUR WORLD.
- Customers require evidence of resilience capability

Managing Expectations

- Management requires metrics and reporting against requirements on capability
- Business leaders require evidence that ‘we have their back’
- Technology leaders require evidence of what is compliant and what is not

Reducing frequency and impact of failures

- Measure impact of outages - NIS Framework – availability in lost user hours
- Important Business Services - Impact Tolerances
- Understanding risk - business analysis and mapping, contract and supply chain management of third parties,
- Problem anticipation and management – eg forensic incident and failure analysis, preventive maintenance
- Introducing change - methods for testing upgrades in 24/7 operation
- Resilience by design - compartmentalisation to localise failures