Information Risk Management – Seminar 4: DR, System Design & Future Trends

Outline:

- Announcements
- DR & BCP
- System Design 101
- Reading & Qestions
- Questions & Next Week

Announcements:

- Final Report:
- → Word Count
- → Address each deliverable
- → Spell check & review
- Refection:
- → Drawn from NOT whole Portfolia
- → Delivery mechanism – Vlog or Report
- → Word Count

How does BCP and DR Support Security?

- Business Continuity Plan / Disaster Recovery (Plan)
- Security Pillars:
- → CIA triad (Confidentiality, Integrity & Availability)
- BCP and DR directly support Availability

Disaster Recovery Plan Elements:

- Definition: Restoring and maintaining communications of technology infrastructure and data.
- → IT Recovery Strategies
- → Internal strategies
- → Dealing with 3rd parties
- Data Backup / Recovery Strategies
- → On-Premise
- → Off –Premise
- → Image Recovery
- → Critical File / Version Recovery
- Physical strategies to maintenance the company system

Disaster Recovery:

- Recovery Time Objectives (RTO)
- → < 15 min to >48 hrs
- Recovery Point Objective (RPO)
- → < 5 min to >24 hrs
- → RTO and RPO main objectives
- Business Impact Assessment (BIA)
- DRaaS (DR as a Service)
- → On Prem -> Cloud (IaaS or Cloud Native?)
- → Infrastructure As Code (IaC)

Business Continuity Plan Elements:

- Definition: Business continuity is about having a plan to deal with difficult situations, so your organization can continue to function with as little disruption as possible.
- Core elements:
- → Business Impact Analysis
- → Recovery Strategy
- → Planning
- → Testing , Simulations → Great way to estimate potential hazard situations
- → Training

Benefits of DR and BCP:

- Reduced risk
- Process improvements
- Improved organisational maturity
- Improved availability and reliability
- Marketplace advantage → Ability to counteract disaster situations

BCP and DR Differences and Similarities:

- BCP is a part of DR
- BCP:
- → Activities required to ensure the continuation of critical business processes in an organisation.
- → Alternate personnel, equipment and facilities.
- Often includes non-IT aspects of business.
- DR:
- → Assessment, salvage, repair and eventual restoration of damage facilities and systems.
- → Often focuses on IT systems.
- “BCP is the umbrella and the DR is under the umbrella”

Elements of Maintaining DR/BCP:

- Simulation Exercises
- → Simple Data Loss
- → Catastrophic Simulation
- Testing
- Training
- Advanced Learning
- 3rd Party Audits

System Design 101:

- Three Tier Architecture
- Resilience
- Network Security
- Cloud Provision / Lock-in

The Three Tiers of Cyber Security:

- System infrastructure for cyber security is commonly divided into three tiers of infrastructure that breaks it down into separate silos presentation, applications processing and data management
- → 1. Presentation Tier: The top tier is a user interface that presents direct access to services in an easy-to-read display. It interfaces with all the other tiers of the network, including the browser/client layer.
- → 2. Domain Logical Tier: The 2nd tier controls functions of the architecture, such as applications processing and business rules. It can be organized as a web server integrated with a web application and / or database server. The logical tier is where cyber security managers have access to establishing and adjusting security risk management policies.
- → 3. Data Storage Tier: The 3rd tier comprises data management. It's a tier that allows IT professionals to conduct regular security procedures, such as continuous monitoring for cyber security threats, without affecting set policies of the overall framework, It's where backups can be stored and accessed in the event of a disaster.

Reading & Questions (Case Study)

- The NSA list a series of 'hard problems' that "required (security) science as a community to focus (on) and measure their progress" (NSA, 2020). These problems concern:
- 1. Scalability and composability
- 2. Policy governed secure collaboration
- 3. Security metrics driven SDLC
- 4. Resilient architectures
- 5. Understanding and accounting for human behaviour (NSA, 2020).

Case Study (Douglas Millward): Example of a Compostable system

- Illustration of the hot topics (scalability and compose ability)
- Cloud server lend themselves very well to compose ability and focus on the idea of taking fixed function blocks and putting them together.
- Web, App and DB server are three functional blocks and can be joined together by compose ability (cloud).
- Tool Apache Brooklyn is a cloud orchestrator, it allows to create cloud systems in a graphical way and hybrid cloud systems
- Problem if AWS used the company is depending of the service and if it goes down, there is no more DR.
- Apache Brooklyn enables flexibility
- → Cloud Orchestrator (e.g. Apache Brooklyn) → OASIS DLS Specification (e.g. TOSCA) → DSL Parser → Functional blocks extracted from specification→ Logical Reasoner & Recommender → Feedback to user based on engine evaluation → User uses feedback to improve design

Reading & Questions – Terje Avaen

- 6/ Available Frameworks and Perspectives:
- → In intergrational decision-making situations, what are the available frameworks and perspectives to be taken? What are other options? When are different frameworks more appropriate than others?
- 7/ Past vs. Future Knowledge:
- → How do we capture the key knowledge issues and uncertainties of the present and future? What duty of care do we owe to future gerneartions? Method: forecasting
- 8/ Risk Assessment Representation:
- → How can we describe and present the result of risk assessments in a way thath is useful to decision-markers, which clearly presents the assumptions made and their justification with respect to the assumptions made and their justification with respect to the knowledge upon which the assessment is based?
- 9/ Risk Information Misrepresentation:
- → How can we display risk information without misrepresentation what we know and do not know ? – How can we accurately represent and account for uncertainties in a way that properly justifies confidence in the risk results?
- 10/ Expert Judgement Quality:
- → How can we stat how good expert judgements are, and how can we improve them? – In the analysis of near-misses, how should we structure the multi-dimensional space of causal proximity among different scenarios in order to measure “how near is a miss to an actual accident”?
- 11/ Real Options Theory & Risk Management
- 12/ The Future of Enterprise Risk Management
- 13/ Machine Learning and Risk Management

Wiki Task:

- Chose ONE of the questions we have discussed / listed in the reading section of this seminar and create a Wiki entry explaining what it means. Put your name next to the entry.

Questions & Next Week:

Remember:

- Report – check all sections answered
- Reflection
- Complete the Feedback Questionnaire