Case Study #2:

Integrating Disaster Recovery /

IT Service Continuity with Information Technology

Governance Frameworks

DeBora King

CSIA 350 7980

Cybersecurity in Business and Industry (2172)

January 29, 2017

INTRODUCTION

The office of the Chief Information Security Officer is not a revenue generating division. Executives across the board may wonder why so much is invested in the areas of disaster recovery and business continuity where there's no return on investment. According to Forbes, businesses expended an average of $686,000 per hour while going through downtime (LaPedis, 2015). The office of the CISO is designed to ensure that uptime is at its maximum and data loss is at its minimum (Alton, 2016). The division is also designed to keep productivity at its highest potential amid potential perils. Since our team members are already aware of the business continuity planning (BCP), business impact analysis (BIA), and continuity/recovery strategies as far as having restore and backup components in place, the objective of this document is to specifically address the functionality of the CISO area regarding the strategic aspect of disaster recovery and business continuity planning. This includes strategic aspects of disaster recovery/business continuity (DR/BCP) planning, implementation and execution.

ASPECTS OF CISO FUNCTIONAL AREA

Disaster Recovery Planning: Planning a strategy for disaster recovery is the most important aspect of the process. It lays the groundwork for compiling a step by step plan for bouncing back from a potential business interruption. The disaster recovery strategic plan's foundation is based on the team assessing critical systems (from the highest priority to the least critical), and in addition, connecting the dots to what is required to make systems operable again in the most minimal downtime. A quote from the ISO standard for IT disaster recovery (ISO 27031) explains it best – "Strategies should define the approaches to implement the required

resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place" (ComputerWeek, 2011).

Disaster Recovery Implementation: A disaster recovery implementation strategy entails defining the company's major assets such as network systems (hardware and software), accounting, critical files, physical and intellectual property, and human resources; identifying threats such as natural disasters (fire, weather storms, or earthquakes) and man-made perils (human error, terrorism, explosion, bio-hazards, epidemic/pandemic, theft/vandalism, business interruption or riots); and response to these emergencies in protecting people, property, and the environment (e.g., coordination of activities such as evacuations, shelter in place, communication, and an alternative worksite) [Ready.gov, n.d.].

Disaster Recovery Execution: There's a saying about how to get to Broadway – the answer: Rehearse, Rehearse, Rehearse. This is the case with the strategy for executing a disaster recovery/business continuity plan. Richard Long of MHA Consulting recommends exercises that involve testing, going through the steps of the strategic disaster recovery plan in detail and in a disciplined timely fashion. He also recommends validation which will help the company identify what does and does not work. (2017).

REQUIREMENTS/IMPLEMENTATION STRATEGIES

According to Ram Mohan of the CISO Platform (June, 2013), Disaster recovery/IT service continuity planning functions performed by staff members in the office of the CISO should include the following:

IT Service Continuity Planning Functions:

- Identifying process specific Recovery Time Objective (RTO)

- Identifying minimum capacity requirement to run the business operations at an acceptable level
- Calculating recovery efforts based on RTO
- Reviewing Service Level Agreements between the organization and external partners
- Identifying critical information resources
- Prioritizing resources in order of recovery
- Identifying procedure for acquiring critical resources in the event of disaster
- Identifying contact information and procedures for disaster authorities
- Identifying and keeping ready a disaster recovery site
- Conducting a cost benefit analysis of moving the business processes to a disaster recovery site
- Defining standard procedures for response, recovery and restoration
- Developing procedures for relocating the business processes to a disaster recovery site
- Defining emergency response procedures that are 1) time based; 2) team based; 3) checklist based; and 4) chronological
- Identifying emergency response team members with contact information
- Creating response, recovery and restoration processes for security and safety
- Documenting and training crisis communication procedures

Restoring IT Services: Specific to restoring IT services that supports critical functions of the business as identified in a business impact analysis (BIA), FEMA suggests a recovery strategy as follows (Rezler, 2014):

- Physical environment where data/servers are housed with climate control, fire suppression systems, alarm systems, authorization and access security. The goal is to have information systems available for restoration, recovery and testing to get everything up and running again.
- Hardware, which includes networks, servers, devices and peripherals
- Connectivity – providing restoration of connections with fiber, cable, and/or wireless components.
- Data and restoration – restoration of software applications critical to the business and assessing the recovery point and time (known as Recovery Point Objective [RPO] of the moment the data should be recovered.

BEST PRACTICES

Control objectives for information and related technology (COBIT) is a framework created by Information systems Audit and Control Association (ISACA). Specific aspects of this framework include connecting the control requirements in response to disaster recovery and business continuity strategies. It also includes policy developments and is a big component of regulatory compliance. What qualifies the COBIT framework mostly is that it is a big component of regulatory compliance, as it helps with Sarbanes Oxley compliance. Companies like ORACLE, UNISYS, and the US Department of veterans Affairs take pride in this framework for their overall improvement of governance and management of enterprise IT.

REFERENCES

LaPedis, R. (2015, February 18). *IT professionals think information security and disaster recovery should be last to get budget cuts*. Forbes. Retrieved from http://www.forbes.com/sites/sungardas/2015/02/18/it-professionals-think-information-security-and-disaster-recovery-should-be-last-to-get-budget-cuts/#7cd9974fe070

Alton, L. (2016, June 1). *Why every small business needs a backup and disaster recovery plan*. Entrepreneur. Retrieved from https://www.entrepreneur.com/article/275473

ComputerWeekly.com. (2011, July). *Developing a disaster recovery strategy and detailed DR plans*. Retrieved from http://www.computerweekly.com/podcast/Developing-a-disaster-recovery-strategy-and-detailed-DR-plans

Department of Homeland Security. (n.d.). *Implementation*. Ready.gov. Retrieved from https://www.ready.gov/business/implementation

Long, R. (2017, January 16). Disaster recovery strategy execution, or will it really work?. MHA Consulting. Retrieved from https://www.mha-it.com/2017/01/disaster-recovery-strategy-execution/

Mohan, R. (2013, June 6). Disaster recovery and business continuity management. CISO Platform. Retrieved from http://www.cisoplatform.com/profiles/blogs/disaster-recovery-and-business-continuity-management

Rezler, R. (2014, March 25). Disaster recovery: steps in a business continuity plan. OnLine Tech. Retrieved from http://resource.onlinetech.com/disaster-recovery-steps-in-a-business-continuity-plan/