Risk and Planning Strategies

Instructor: Risk is an inherent part of business that cannot be eliminated. The best an organization can do, is reduce its risks to a level that is reasonable or acceptable - their risk appetite. Finding that optimal point of acceptance takes some analysis to determine where cost of loss intersects with cost of mitigation; what is spent to mitigate a risk, shouldn't exceed the cost of loss. Recall the old thousand-dollar fence around a stack of quarter analogy.

Types of risk include: Aggregate: when a threat affects a large number of vulnerabilities, which combined have a significant impact. Inherent: risk linked to a particular activity. Control: results from a failure of controls to properly mitigate risk. Residual: risk that remains after mitigating controls have been applied.

Risk assessments identify current threats, vulnerabilities, and risks residing in the enterprise. It prioritizes potential business disruptions based upon severity, likelihood of occurrence, and impact of given threats.

Assessing risks is a process performed regularly at the organizational, system and application levels. Vulnerability and penetration testing tools aid in

assessments by identify weaknesses in the enterprise; And structured risk assessment frameworks provide guidance on conducting.

Risk analysis is often a component of assessment. It examines loss and exposure variables to formulate meaningful information that decision makers can use to prioritize specific risks and mitigation resources.

Qualitative analysis levels risk based on likelihood and potential consequences. Quantitative analysis applies numerical values to impact and loss value of a specific asset or function.

Gap analysis compares the current state of the enterprise, to the desired state after improvements or mitigations, in order to highlight the gap between the two.

Even with the most careful analysis and implementation of controls to mitigate risks, threats can still be realized. Business impact analysis is a means for determining the impact should an adverse event occur. B-I-A requires an intimate understanding of all business components, and which are critical to establish priorities for recovery solutions.

Impacts to People, Information, Technology, and Facilities are considered as well as supporting elements that are critical to operations.

Key goals of business impact analysis are: Recovery time objective - the amount of time a business can function without the process. Recovery point objective - the amount of data that will be restored if lost in an outage. Maximum allowable outage, downtime - the length of time the business can tolerate; their maximum tolerable period of disruption.

There are challenges with risk assessments and analysis. Assessing the cost of an attack can be difficult. Predicting when and how an attack will occur is unlikely. The pace technology and systems evolve, and in turn new vulnerabilities, will cause data on risk factors to be limited and become outdated. When data analysis is not precise, maintaining alignment to business objectives and continuity of critical functions will aid in deconflicting priorities.

Business continuity management considers critical functions and identifies strategies to protect them from the effects of a disruption. The business continuity plan may reflect a specific process, or address all key processes. There are several plans that are commonly components of a business continuity plan. These supporting documents formalize procedures during a disruption such as: relocating and recovering critical functions, communicating status to internal and external stakeholders, and personnel guidance and roles. Business continuity planning, a full-spectrum enterprise strategy

minimizing loss and resuming operations in the event of a disruption, significantly improves the survivability of an organization.

Business impact analysis is used to differentiate between the most critical functions of an organization. The activities include: Performing risk or threat analysis to determine the risks that should be accepted, transferred, or mitigated. Defining the critical business processes, dependencies, and priorities. Considering legal, regulatory, and contractual obligations. Understanding third-party dependencies and the management succession plan.

Business continuity planning should be periodically tested to ensure the strategies and procedures developed to ensure critical operations resume in the event of a failure or disruption, are effective.

While continuity planning is resuming operations in the event of a failure or disruption, disaster recovery planning details how to restore operations after a disaster like a fire or flood, major outage events.

It's not only the facility and network infrastructure considered in a disaster, there are non-technical elements as well: People, and their specific needs. Utilities, power, and HVAC. Logistics of how the plan will be executed; who is in charge of which element, how will communications with teams work?

And also agreements - the contingency contracts with other parties to aid recovery following a disaster.

Backups are critical in the event of disaster. Backups of all original information including data in electronic and paper form. Considerations for backups include: Backing up everything - data, source code license keys. Tier the data based on importance and frequency of need. Where to physically store backups for confidence in the availability if needed. Backup equipment configurations. Encrypt the backup data to secure it just as the originals are. Be sure to test the ability to restore from the backups, and ensure it meets recovery time or recovery point objectives.

Removing single points of failure aids in quick recovery. This applies to equipment, personnel, or any single source dependency. For instance, you don't want a single firewall administrator. Should something happen to that person where they're no longer available, or similarly if a single firewall is inspecting network traffic, the failure of that device would be detrimental.

To address this, redundancy and fault tolerance is built in. Redundancy such as backups, additional alternates, for business functions; creates fault tolerance where operations can continue despite an outage. Diversity is valuable here as well. For example, if an identically

configured server is the backup for the primary, an application vulnerability in a version they're running, would affect them both. For assets and functions that are critical, high availability is ensuring any vulnerabilities that would cause failure are addressed. Solutions include RAID where backups of backups are created, redundant services, hot swaps for quick restoration, or an alternate site that mirrors functionalities.

The type of alternate site for continuing operations in the event the main location is unavailable, depends on tolerable downtime, and cost-benefit analysis. Having multiple processing centers will limit downtime, involves transferring work load. A mirrored site, having an exact copy of the primary site is costly, but minimal downtime. A hot site is fully equipped, but not an exact mirror, requires some restoration time. A Warm site is partially equipped, and will requires setup time. Cold site is a bare minimum, non-equipped, location and there are also mobile units where equipment is delivered for temporary use.

Understanding critical business objectives, and what could cause harm or cause interruption, will help define mitigation strategies. Business continuity and recovery planning can limit downtime from an outage or disaster, to resume operations in a timely manner and minimize loss.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098