RISK ASSESSMENT GUIDELINES

A Risk Assessment is a business tool used to gauge risks to the business and to assist in safeguarding against that risk by developing countermeasures and mitigation strategies. The Risk Assessment Process is the important first step in Business Continuity and Disaster Recovery planning projects.

There are two types of Risk Assessment: Qualitative and Quantitative. An organization can elect to perform one of the two or both of the types of assessment. Both approaches match threat levels to vulnerabilities in the business operation and attempt to mitigate the associated risk with that matching.

A Qualitative assessment assigns risk on a level rating from high to low, whereas a Quantitative assessment assigns a monetary value to the level of risk. The Quantitative assessment requires a higher degree of knowledge of business operations to accurately reflect the data needed to perform the risk assessment calculation. Most organizations perform the Qualitative assessment first, and then use it to complete the Quantitative assessment. An example of the Risk Assessment Report can be found at the end of this document.

A. Qualitative Risk Assessment

The process to completing a Qualitative Risk Assessment is detailed and requires the assessor to consider all of the following steps.

1. The business system must be characterized completely

In order to assess risk to an asset or business system, the system must be fully understood by the assessor. All aspects of the system should be documented by the business officer who is responsible for that portion of the system. The assessor should evaluate this documentation against observation of the system to complete the description of the system. To characterize the business system, all of the following factors must be considered:

- System Hardware/Software
- System Interfaces (Internal/External)
- System processes
- System usage and data sensitivity
- Staff using the system and purpose
- Functional requirements of the system
- System security policies
- System security architecture and network topology
- Data retention and disposal techniques
- System data flowcharts
- System Technical, Operational, and Access Controls
- Physical and Environmental security for system

The result of step 1 should yield a detailed description of the business or IT system.

2. All potential vulnerabilities to the system must be identified

A vulnerability is defined as a weakness that can be accidentally triggered or intentionally exploited against a business system. A primary goal of the Risk Assessment Process is to identify, in order to eliminate or mitigate, potential vulnerabilities to the system. Vulnerabilities could range from inactivate user accounts for terminated employees or programming code vulnerabilities that allow hackers to penetrate the system for malicious use (non-technical to technical). Vulnerabilities vary from system to system; however, considerations should be made for the following:

- OWASP Top Ten Web Application Security Flaws (available from http://www.owasp.org) – details the most common security flaws that have been used to exploit systems for the stated year.

- National Vulnerability Database (http://icat.nist.gov) –details all known system vulnerabilities in a searchable database.

- System Network and Application Layer Penetration testing—penetration testing into system vulnerabilities can be used to detect technical flaws that are specific to the organization. Automated tools exist for this technical testing; however, the reliability of automated tools is questionable due to diversity in systems and will produce false-positives.

- Non Technical vulnerabilities can be detected through social engineering and coercion on the part of the assessor in the attempt to obtain unauthorized information from staff.

The output from step 2 should yield a list of system vulnerabilities that can be used given a threat source.

3. All potential threats to the system must be identified

A threat is the potential for a threat-source to successfully exploit a vulnerability. A threat-source is defined as the method that triggers a vulnerability, whether by accident or by malicious intent. Common threat-sources to consider while determining all potential threats to the system are:

- Natural threats such as floods, earthquakes, heavy storms, fire, etc.
- Human threats such as unauthorized access to secure systems, incorrect data entry, etc.
- Environmental threats such as chemical contamination, pollution, power failure, HVAC failure, etc.

A list of all organizational threats should be readily available to all IT and other staff in order to quickly address both accidental and malicious threats that are specific to that business system.

The output from step 3 should yield a list of threats that can be used against the vulnerabilities identified in step 2.

4. Detail established countermeasures for known threats

This step requires that the assessor review the existing countermeasures for known threats and describe those countermeasures. Countermeasure controls are both technical (computer hardware/software controls) and non-technical (management and operational controls). Controls should be categorized as either:

- Preventative Controls – preemptively work to stop threats from exploiting system vulnerabilities
- Detective Controls – warn of violations of security policy through checksum monitors, intrusion detection methods or audit trails.

The output for step 4 should be a list of current organizational countermeasures to mitigate known vulnerabilities.

5. The assessor must determine the risk level (impact analysis)

In this step the adverse impact of a threat to the system is determined. The system mission, data criticality and data sensitivity are considered in the impact analysis. Many organizations refer to this as a Business Impact Analysis, where impact levels are prioritized based on the sensitivity and criticality of the asset if a compromise were to occur. Impact analysis is also referred to as loss analysis, because it is qualitatively addressed by loss of: integrity, availability and confidentiality.

- Loss of Integrity: If the system no longer protects against unauthorized modification, loss of integrity of the data has occurred. Loss of data integrity can lead to inaccuracy, fraud or poor decision-making for business operations. It can also adversely affect the availability and/or confidentiality of the data.

- Loss of Availability: If the system is inaccessible to users, business productivity and/or sales can be impacted. This can affect revenue, customer loyalty and business presence.

- Loss of Confidentiality: If the confidentiality of the system data is compromised, the business may have legal and industry regulatory consequences, in addition to loss of public confidence and loss of revenue.

The impact/risk level is assigned as High, Medium or Low for each risk area for a given asset. The definitions of the impact levels can be characterized as:

- High: Exploit of the vulnerability whereby (1) high cost loss of major tangible assets or resources is realized, (2) causes harm to the organization's mission and reputation , or (3) causes human death or serious injury.

- Medium: Exploit of the vulnerability whereby (1) cost loss of a tangible asset or resource is realized, (2) causes harm to the organization's mission and reputation, or (3) causes human injury.

- Low: Exploit of the vulnerability whereby (1) loss of some tangible assets or resources is realized, or (2) may cause noticeable impact on organization reputation.

The output for step 5 should be a magnitude rating (high, medium, low) for the impact of an exploit against an assets (resource) vulnerability.

6. The assessor must determine the likelihood of an incident to the system

The likelihood of an incident is evaluated by considering the following factors: Threat-source motivation, characterization of the vulnerability, and effectiveness of existing countermeasures. The likelihood is categorized as a rating of high, medium or low:

- High: threat-source is highly motivated and countermeasures are ineffective against the threat.
- Medium: threat-source is motivated and countermeasures may be effective against the threat.
- Low: threat-source is not motivated and countermeasures are effective against the threat.

The output for step 6 should be a risk rating of high, medium or low for the likelihood that a threat-source will exercise a threat against a system vulnerability.

7. Additional countermeasures to offset the determined risk must be identified

Because the existing countermeasures evaluated earlier in the Risk Assessment process might not be effective against threats identified during the Risk Assessment process, additional countermeasures are suggested as part of the process. All countermeasures should be evaluated on a cost-benefit basis before development/implementation.

The output for step 7 should be a list of recommended new countermeasures for threat sources identified during the Risk Assessment process.

8. The results of the Risk Assessment are documented by the assessor and distributed to all business officers

The assessor prepares a Risk Assessment Report to document all findings and produce the final Risk Assessment rating or value. An example of a Risk Assessment Report can be found at the end of this document. The Risk Assessment report can contain elements of qualitative and quantitative risk analysis. The more detailed the report, the better an organization can safeguard against potential threats.

B. Quantitative Risk Assessment

The process to completing a Quantitative Risk Assessment is similar to the Qualitative assessment, only differing on steps #5 and #6, where a monetary value is calculated for the likelihood of an incident and the level of risk facing the organization.

In order to calculate the risk loss in monetary terms, three calculations are required.

1. Determine the SLE (Single Loss Expectancy) for a given asset. The SLE is the difference between the asset's original value and the estimated value remaining after a single exploit to that asset. **SLE ($) = asset value ($) * Exposure Factor (%)**, where the exposure factor is an estimate of the loss of availability of the business asset due to an exploit. The exploit could be data loss, natural disaster, theft, alteration or a malicious data exploit to an IT system. *(This is Step 5 in the Qualitative Risk Assessment.)*

2. Determine the ARO (Annual Rate of Occurrence) for the asset as a percentage. The ARO is the probability of that a threat event will be successful over a period of a year. For example, if the business is located in a geographic area prone to earthquakes, the ARO of an earthquake damaging business assets could be 20% based on trend analysis of previous years earthquake rate. *(This is Step 6 in the Qualitative Risk Assessment.)*

3. Determine the ALE (Annualized Loss Expectancy) for the asset as a monetary value. The ALE is the estimated value that a business entity should invest for countermeasure activity against risks to the asset. **ALE ($) = ARO (%) * SLE ($)** for a given asset.

By totaling the ALE for each asset the business determines is essential to safeguard, an organization can determine the cost of securing business continuity resources OR determine that most cost effective mitigation strategies may be needed.

A simple example of the Quantitative Risk Assessment calculation is below:

- Bob and Jane have purchased a new house for $100,000.00 on the coast. Bob estimates that if the house is in the path of the storm, up to 50% of the house could be damaged without being a total loss. (If the house was a total loss, SLE would = $100,000.00)
    - SLE = $100,000.00 * 50%
    - SLE = $50,000.00

- The average rate of hurricane activity for their region is 2.2%, based on 22 hurricanes making landfall in that area over the past 10 years. (ARO).

- Jane wants to make sure that their savings could be used cover any damage to the house in the event of a hurricane, so she calculates the annual loss expectancy if their home was 50% destroyed by a hurricane.
    - ALE = 2.2% * $50,000.00
    - ALE = $1,100.00
    - Jane and Bob's mitigation strategy thus includes adding $1,100.00 to their savings account a year in the event of a disaster to their home.

C. Risk Assessment Reporting

RISK ASSESSMENT GUIDELINES

The Risk Assessment Report contains all the findings of the risk assessment and is used to assist management in Business Continuity and Disaster Recovery planning. A sample Risk Assessment Report is below. **Remember that the Risk Assessment Report is a confidential business document that should not be made public.**

Widget Department
Risk Assessment Report

Introduction

This risk assessment will detail both qualitative and quantitative risks to Widget department. Data was gathered by the IT and business officers to complete this report via internal procedural documentation, observance, and employee interview. This risk assessment will be based on the system at the primary operating location. The system at the secondary location is identical to the primary location and is designed to be used in the event that a disaster at the primary location occurs.

System Summary

The Widget Datacenter contains three physical servers, one of which is the fail-over node and is not used in daily operation. All three machines have virtualized environments that can sync between the physical machines for fail-over purposes.

Machine A hosts the Widget department's inventory/customer management system. The 3 Virtual Machines (VMs) are divided thusly: The $INVEN VM contains the internal inventory/customer management application for staff to use to manage warehouse inventory and process customer orders, the $DATABASE VM contains all databases needed for the inventory/customer management system, and the $WEBSALES VM hosts the website used by customers to shop online for Widget products.

Machine B hosts the online payment system, separated into 3 VMs: The $CCWEB VM has the web interface for customers to pay for online orders by credit card, the $CCDB VM houses the databases needed to support the online payment application, and the $CCAPP VM hosts the application used by staff to manage payment data and also to process walk-in or telephone orders for customers.

All machines have a backup agent for OffSiteBackup.Com installed where data is synced to the backup storage location dedicated to Widget Department's data. Data is encrypted at the backup location and can only be decrypted during the restore process to a Widget Department machine. Backup data can be restored by designated Widget department staff at any time. In addition, all data is mirrored to the equipment at the secondary location via the backup agent of the virtualization software.

All machines are behind a firewall UTM device that separates the web VMs into a DMZ to maximize protection for the database and application machines. Staff access the applications by logging into each assigned system using the Firewall SSL VPN tunnel. The firewall is connected to the broadband modem provided by the Ethernet Provider.

The Primary and secondary facilities contain the following equipment (model and serial numbers for all equipment is recorded in the Accounting module of the inventory management system):

1. 10 – Dell Vostro 320 FT10 workstations
2. 3 – HP LaserJect P1505N network printers
3. 2 – Dell PowerEdge M905 servers with a total of 6 virtual machines
4. 1 – Netgear ProSecure UTM25
5. 1 – HP 3180 Fax
6. 1 – Canon ImageCLASS D1105 copier
7. 4 – IBM SurePOS 300 Express cash registers

System Vulnerabilities Defined

The vulnerabilities to the information system described above could include all of the following:

- Web Code vulnerabilities
- Access to the Data Center
- Poorly configured Firewall
- Malicious software on employee workstations
- Password management on registers
- Secondary location access restrictions
- Flaws in vendor software/equipment
- Access to Administrator credentials on servers

System Threats Defined

The threat sources associated with the above vulnerabilities are listed below:

- Web Code vulnerabilities – Both physical machines have web code to support the online store and online payment engine for Widget Department. Web code in general is vulnerable to human threat for hacking.

- Access to the Data Center – The Data Center is vulnerable to unauthorized access by Widget employees or external personnel. Once in the Data Center, serious harm could be inflicted on critical systems.

- Poorly configured Firewall – Poor configuration of firewall resources could allow malicious software to infect the physical servers or fail to protect against a Denial of Service attack against the Widget Department's online presence.

- Malicious software on employee workstations – Malware on employee workstations can compromise the integrity of data and perhaps permit unauthorized access to the servers.

- Password management for registers and workstations –Password management on registers and employee workstations is a manual process and could be subject to human error.

- Secondary location access restrictions – Because the secondary facility is "dark" unauthorized access to the facility could become an issue.

- Flaws in vendor software/equipment – If vendor software/equipment is not patched for vulnerabilities, this could leave the system open to hacking attacks.

- Access to Administrator credentials on servers – If the administrator credentials on the servers were compromised, the entire system would be vulnerable to data theft.

Countermeasures for known threats

The in-place countermeasures for the above threats are listed below:

- Hacking or Malicious Software Injection Attempts: To preventatively counteract any hacking or malicious software injection attempts, the Netgear UTM device is configured to only allow public access to the DMZ for $CCWEB and $WEBSALES for customer self-service orders and payments. Access to internal LAN systems is only permitted from Widget Department registered machines and via the Netgear VPN. The employee workstations are "locked-down" and are not given email client access or Internet access. In addition, each Widget Workstation is remotely scanned using an industry-recognized Vulnerability Scanning tool nightly to safeguard against hacking attempts. Only the Widget Webmaster has access the Widget email account and to the Internet. This machine is not permitted to access server objects within the internal LAN.

- Password Complexity: Passwords are required for employees to login to Widget workstations every day. The IT team retains administrator privileges to all workstations and configured the Windows OS on all workstations to expire passwords every 90 days. Incorrect login credentials will lock the user from accessing the workstation as well. IT staff have to manually unlock the user at the workstation. Widget department is looking into biometrics for machine access.

- Facility Controls: The secondary facility is a "dark" facility, with no daily human presence. The Data Center environment and power controls are all automated. The primary Data Center is also automated. Entry into the Data Center is controlled with biometrics; however, entry to the facility is managed with standard key entry. If power disruptions occur, the Data Center entry point fails-locked. At this point, the IT manager, Business Office manager, Accounting Office manager and Personnel Manager must all be present to override the system to open the door. The facility UPS functions long enough to initiate the virtualization software data migration to the secondary system. Both facilities are monitored by security camera and alarm systems. If forced entry occurs, the alarm security notifies law enforcement immediately.

- Unauthorized System Access: To combat the use of Administrator credentials by unauthorized users, no human is permitted to login to the servers as Administrator and all services are assigned individual credentials. All server credential passwords are expired and changed every 2 months.

- Human Error/Lack of Training: Employee misuse of system resources can cause a breach of data, or influence the integrity of data. To combat employee misuse, Widget Department holds mandatory annual training for system usage policies/procedures and any industry or legal regulations that are applicable to the job. New employees are trained prior to the granting of system access.

- Vendor Support: Lack of vendor support for devices, such as firewalls, could lead to device vulnerabilities that would be beyond Widget Department's control. The IT team remains in constant contact with all vendors and monitors reliable sources of newly discovered threats in order to verify that 3rd party equipment is quickly patched by the vendors. Any vendor that lapses on critical updates is immediately contacted and in past cases been dropped as a Widget Department vendor.

Determination of Risk Level (Impact Analysis)

This Risk Assessment will describe risk to the system in both Qualitative and Quantitative methods. The Qualitative method assigns a level: high, medium or low based on the system threat sources and the level of damage that those threat sources could cause. The Quantitative method derives the risk level as a monetary value (Single Loss Expectancy) - based on the value of the asset and the estimated loss of the asset should an incident occur.

Qualitative Impact Analysis
Based on the system design and the vulnerabilities/threat sources to the organization, the Qualitative Impact to the business is **LOW**. An incident or disaster to the Widget Department's system would be recovered quickly by immediate fail-over to the secondary system. Estimated customer impact is minuscule. If the primary system is destroyed, cost to replace the system can diffused long-term while the secondary system is operational.

Quantitative Impact Analysis
The Single Loss Expectancy (SLE) for each asset in the server environment is listed below. Equipment with a total cost of less than $1,000.00 will be excluded from the calculations. The SLE is derived from the asset's total value multiplied by the Exposure Factor, which is the estimation of the loss of business availability during a disaster or incident.

The SLE for each component will be arranged under the following vulnerability outcomes:

Asset theft or destruction – the estimated exposure factor for this occurrence is 20%, based on facility entry and preventative controls.

1. 2 – Dell PowerEdge M905 servers
   Each server value is $7,500.00 for a total value of $15,000.00
   SLE = Value ($15K) * Exposure Factor (20%)
   Server SLE = $3,000.00

2. 1 – Netgear ProSecure UTM25
   The UTM value is $5,000.00
   SLE = Value ($5K) * Exposure Factor (20%)
   UTM SLE = $1,000.00

3. 4 – IBM SurePOS 300 Express cash registers
   A register value is $1,000.00 for a total value of $4,000.00
   SLE = Value ($4K) * Exposure Factor (20%)
   Register SLE = $800.00

TOTAL SYSTEM SLE FOR THEFT/DESTRUCTION = $4,800.00

Data compromise – the estimated exposure factor for this occurrence is 50%, based on access control complexity and employee misuse prevention.

1. 2 – Dell PowerEdge M905 servers
   Each server value is $7,500.00 for a total value of $15,000.00
   SLE = Value ($15K) * Exposure Factor (50%)
   Server SLE = $7,500.00

2. 1 – Netgear ProSecure UTM25
   The UTM value is $5,000.00
   SLE = Value ($5K) * Exposure Factor (50%)
   UTM SLE = $2,500.00

3. 4 – IBM SurePOS 300 Express cash registers
   A register value is $1,000.00 for a total value of $4,000.00
   SLE = Value ($4K) * Exposure Factor (50%)
   Register SLE = $2,000.00

TOTAL SYSTEM SLE FOR DATA COMPROMISE = $12,000.00

Likelihood of Incident

The likelihood of an incident is determined by measuring the known threat sources vs. the existing countermeasures in place. This is known as the Annual Rate of Occurrence (ARO).

Asset theft or destruction –
Based on current countermeasures the ARO for asset theft or destruction is estimated to be 10%.

Data compromise –
Based on current countermeasures the ARO for data compromise is estimated to be 20%

After determining the ARO, the Annual Loss Expectancy -ALE- can be calculated (for a Quantitative Risk Analysis) by multiplying the SLE to the ARO. The ALE provides the organization a monetary goal for recovery costs. By taking the total SLE for the above vulnerability outcomes, Widget Department has determined the ALE for both outcomes as follows:

Asset theft or destruction –
ALE = SLE ($4,800.00) * ARO (10%)
ALE = $480.00

Data compromise –
ALE = SLE ($12,000.00) * ARO (20%)
ALE = $2,400.00

The total annual monetary goal for recovery is **$2,880.00**

Additional Countermeasures

This assessor recommends to Widget Department a few additional countermeasures to reduce the risk level to the organization.

1. Implement two-factor authentication for all staff to login to workstations and for all system access. If an employee’s password is compromised, two-factor can mitigate any data loss.

2. IT staff should be parsing and comparing log activity daily to ensure the system has not been compromised.

3. Implement a file-integrity monitoring system to alert if critical files are modified without proper authorization.

SAMPLE RISK ASSESSMENT REPORT

Summary

This Risk Assessment must be reviewed annually to ensure accuracy for the current state of the system. This Risk Assessment is confidential to the organization and will not be publicized. The assessor ensures the accuracy of this assessment.

____ ______________________
Printed Name Date

____
Signature of Assessor