A Risk Assessment Checklist

For Small Business

Table of Contents

1.0 The Purpose of a Risk Assessment Security Checklists 2
2.0 Where Do I Begin? 2
2.1 Risk Assessment Checklist - A Basic Approach 2
2.1.1 Measuring Confidentiality, Integrity and Availability (CIA) 2
2.1.2 Asset Inventory and Ranking 3
2.1.3 Evaluate Security Policies, Procedures and Technologies 4
3.0 How Much Security, More or Better? 4
3.1 Small Business with Scarce Resources - What to do 5
3.2 Basic Cost/Benefit Analysis 5
3.2.1 Security Threat Gap Document 5
3.2.2 Architecture Cost Estimate Analysis 6
4.0 Conclusion 7

1.0 The Purpose of a Risk Assessment Security Checklists

A security checklist (sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration) is essentially a document that contains instructions or procedures for configuring an IT product to a baseline level of security. Checklists can be developed not only by IT vendors, but also by consortia, academia, industry, governmental organizations and others. The checklist can be broad covering whether a company has a security policy, a business continuity/disaster recovery plan to specific hardening procedures of an operating system. It can even serve a step in the course of conducting a risk assessment that would drive a cost/benefit analysis which I am going to explain in this document.

Computer security is essential to protect from viruses, spyware, hackers, and many other threats including physical security. To ensure you're fully protected, begin by matching your current and future security needs to the required security technologies. It is also important to be in compliance with mandated federal and state laws, as well as industry compliance such as PCI. Ignorance is not bliss, for these mandates are required to be complied with and proven, you are expected to know them. Some state laws such as Massachusetts levy criminal penalties for not being in compliance and most require security breach disclosures to the victims and general public so always be cognizant and proactive because the penalties are severe. A few states have enacted security laws such as Massachusetts, Texas and California with the remainder having pending or considering similar legislation.

2.0 Where Do I Begin?

It all begins by knowing your business, your surroundings and your environment. Computers nowadays are the main tools that support and run the business where the critically important data of any organization resides. It is this data that is stored and transacted upon within computerized systems that needs protection. Your customer data, employee records, financial, legal, trade secrets and other highly confidential information are the life blood of a company.

2.1 Risk Assessment Checklist - A Basic Approach

2.1.1 Measuring Confidentiality, Integrity and Availability (CIA)

In many large organizations risk assessments carry a whole new meaning with departments devoted solely for assessing a corporation's risk of every Information Technology asset conducting both qualitative and quantitative assessments. The difference between the two is one is conducted on a mathematical calculation (quantitative) based on historical security metrics developed in the industry on the type and class of an asset and takes up the most time because of its sophistication. The other (qualitative used in this approach) is a rapid assessment performed in a shorter period of time and with less data. It is more descriptive than measurable, although I am using some mathematics taken from the quantitative approach to measure and rank the asset's risk based on CIA.

Enter the advent of Cloud Computing and yet another set of criteria exists on top of the CIA categories that are required to assess the security risk to data residing and being transacted upon in the cloud, it becomes complex. For the small business, the CIA of data is fundamentally important to understand

that would measure the risk of an asset and a good starting point. The following are the steps on creating a Risk Assessment Checklist:

2.1.2 Asset Inventory and Ranking

1. Conduct an inventory of all your data and classify them from the most important to the least. Assign a number ranking system from 1-3 in the order of importance, 1 being the most important to 3 the least. An example would be classifying them as Confidential (financials, employee records, client and vendor contracts, legal, trade secrets, etc.) Sensitive (internal memorandums, client/vendor communications, SLAs, travel arrangements, etc.) and Non Sensitive (sales brochures, informational web sites, press releases, etc.).
2. Rank the inventoried and classified data assigning a number to each CIA column according to the financial impact it would have and how much trust (integrity) you place in the data as being reliable to the business, if compromised and not being available for a period of time. Understand that any data has a financial impact to a business if Confidentiality, Integrity or Availability is compromised and each should have a number assigned.
3. Sort the data by CIA column order, this will provide the ranking of all your data a key metric to determine the level of risk and security is required to protect the data.

In the illustration below shows a variety of ranked assets comprised of data and applications. The risk score is calculated as the average of CIA, the lower the score the higher risk probability the asset has.

Asset Name	Confidentiality	Integrity	Availability	Risk Score
Financial Data	1	1	1	1.0
Employee Data	1	1	1	1.0
AD/LDAP	1	1	1	1.0
Client Data	1	1	2	1.3
NDA	1	1	2	1.3
SOW	1	1	2	1.3
Email	2	2	1	1.7
Connectwise	2	2	1	1.7
Kaseya	2	2	1	1.7
Vendor Data	2	2	3	2.3
Memorandums	2	2	3	2.3
Client Prospects	2	2	3	2.3
SLA	2	2	3	2.3
Press Release	3	3	3	3.0

2.1.3 Evaluate Security Policies, Procedures and Technologies

Now that the data is inventoried and ranked, the next step is to evaluate your security policies, procedures and technologies protecting the assets that are already in place allowing identification of gaps. This will help determine how many layers of protection your computer security system needs:

1. Do you have a security policy that governs your security framework?
2. Do you have a business continuity/disaster recovery plan?
3. Do you have an access management policy and/or procedures on who can get in and what can they do?
4. Is there an incident management plan/procedure on how to respond to an incident should one occur?
5. Is there a personnel security policy and/or procedure?
6. Do you provide security awareness and training to your personnel?
7. Do you have data protection procedures in place and functional?
8. Does your technical infrastructure have secure transmission of data capabilities and in use?
    a. Are all mobile laptops as well as stationary desktops protected by firewalls, virtual private networks (VPNs), and intrusion prevention?
    b. Are all of your computers protected by antivirus software and is it up to date?
    c. Do all your security tools communicate with one another?
9. Do you have delivery partner management procedures in place?
10. Is your physical infrastructure (data center) secure and environmentally safe?
11. Are you aware and are you in compliance with any mandated law? Are your clients and do you know that they should be if handling their data?
    a. Are you encrypting the most sensitive information and/or mandated by law, i.e. HIPAA, PCI?
12. Do you have service delivery management that provides security competency in services and products provided to your clients?

This are just a flavor of the types of questions used to development a risk assessment checklist and is a step in the risk management process.

3.0 How Much Security, More or Better?

Once the risk assessment has been completed and identification of the gaps, the next thing is what to do about those gaps and close them. A key consideration is what is my return on an investment in a technology and how much security will be returned that would substantially diminish or eliminating the risk. The return on investment (ROI) and the return on risk (ROR) factor into the decision and the company must consider how much security can it reasonably afford to support the business without taking on disastrous risks should breaches occur or forced upon by government and client/vendor

contractual mandates. It is more and more evident that security is now part of the cost of doing business in any organization and must be factored in the business model. It is a key success factor in any organization large or small since it supports and is part of the foundation of operations. The successful management of information security in any organization is vital to its success and survival.

3.1 Small Business with Scarce Resources - What to do

Collecting data has always been a difficult task with regards to information security. With small businesses, personnel resources are scarce to adequately track the number of security breaches that occur annually and the impact to their financials are not documented. Simply put, small businesses do not have the time to devote toward data collection. The problem here is there is no reliable data to make good decisions, conducting a quantified risk assessment is much needed and in demand today in the small business community. Without good historical data collected from their organization and data collected from other small businesses that are comparable, all small businesses are at a loss to proceed with implementing any security project. Many small businesses forgo security improvements and take on unnecessary risks then later suffer the consequences via security breaches or are found not in compliance with federal and state mandates. Some suffer both events and the survival of these businesses is at stake. As previously mentioned one state, Massachusetts, levies criminal penalties against the owners of the business that conducts business in the state. One could easily argue a small business cannot afford not to be in compliance today and not to have in place proven security technologies that reduce or eliminate the risks, a common analogy is "damned if we do and damned if we don't". But it is good business practice to be secure, it is common sense, a frame of mind we often take for granted. We all know most everyone has dead bolt locks on their doors and lock them to prevent intruders from walking into their homes. Some small businesses that do implement security technologies to protect their data always finding problems figuring out the cost structures of these initiatives and how to pass these costs on to their customers.

3.2 Basic Cost/Benefit Analysis

Devising an understandable analysis that weighs the security implementation project can be complex for the small business. Key considerations are threat identification of the gap obtained from the risk assessment discussed above and its impact to the data. Here is one example of a methodology taking an indentified security gap and driving it to a cost/benefit analysis:

3.2.1 Security Threat Gap Document

GAP Number:	AD 1
Name:	Employees gain administrative rights to Accounting Finance
Scope:	Access Management
Priority:	HIGH (HIGH, MEDIUM or LOW)
Environment:	Internal - LAN
Users Affected:	ALL USERS in Active Directory
Access Right Levels:	Administrator full privileges
Entry Point:	At Host
CIA Categories Affected:	Confidentiality , Integrity and Availability 1-1-1 Risk Score 1.0

Threat Description:	All employees can log into and have unauthorized access, segregation of duties violations.
Sophistication:	LOW
Condition:	Users have unintended login rights in an administrative accounting group in Active Directory.
Policy:	Specific users have expressed admin rights to Accounting
Consequence:	Users gain unauthorized access and tamper with configuration and data; confidentiality of data is breached and leaked such as payroll and vital financial data the most severe.
Recommendation:	Remove users not authorized to access accounting and ensure they are placed in their correct access rights groups in Active Directory and monitored for correctness periodically, every quarter.

3.2.2 Architecture Cost Estimate Analysis

The final step is developing a cost analysis in time and materials to remedy the gap. The analysis will contain each identified gap detailing the recommendation detailing implementation, maintenance, hardware and software required costs:

GAP #	Recommendation	Priority	Implementation Annual Costs	Maintenance Annual Costs	Hardware Annual Costs	Software Annual Costs
AD1	Remove users not authorized to access accounting and ensure they placed in their correct access rights groups in Active Directory and monitored for correctness periodically, every quarter.	HIGH	$500	$3,000	$0	$0

In this example it was a fairly easy task to correct an obvious error by an inadvertent grouping of employees to an accounting administration group account. In this case logging can be enabled to ensure that users are monitored in their appropriate groups and access privileges according to their job responsibility. The costs associated is the time to correct the errors by an authorized administrator and set up logging/monitoring of all user accounts and review them periodically for policy compliance.

4.0 Conclusion

The main objective of the Risk Assessment Checklist builds the road and provides data on driving a Cost/Benefit analysis for small business. This information quantifies the financial costs necessary to implement security improvements. Within this framework we inventory all information technology assets and determine its financial impact in the three CIA categories by assigning a ranking order of importance. We identify open and potential security vulnerabilities from a checklist of questionnaires that identify security gaps and document its severity, consequences and recommendation for corrective action. From these corrective actions a cost analysis is determined to remediate the identified vulnerabilities. The overall benefit to a small business is having a less volatility, a more secure and monitored environment that delivers value to the business and to the clients they serve.

Prepared for CompTIA by George Moraetes, CISM, CGEIT