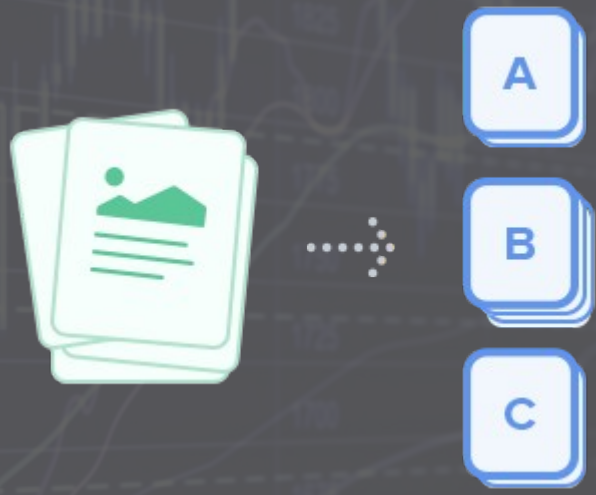
Risk Management: Security Categorization of the Payroll System

A CompanyX White Paper



By Ryan Nye
CSOL 530, Module 2, Version 1
February 2, 2018

Guidance

The beginning of a risk management plan start with categorizing risks by impact on the organization.

Process Inputs:

1. Identify Information Types
2. Select Provisional Impact Levels
3. Review Provisional Impact Levels
4. Adjust/Finalize Impact Levels
5. Assign System Security Category

Process Outputs:

6. Security Categorization
7. FIPS 200 / SP 800-53 Security Control Selection

The following standards provides guidance on how to categorize risks in the payroll department:

PS PUB 199 Standards for Security Categorization of Federal Information and Information Systems

This publication includes:

- Impact levels and definitions for CIA/AIC Security Objectives
- Security Categorization Applied to 1) Information Types 2) Information Systems
- Summary Table of Security Objective and Impact level

The acceptable levels of impact level are LOW, MODERATE, and HIGH. Categories used for a given system:

{(Confidentiality, impact lvl),
(Integrity, impact lvl),
(availabilty, impact lvl)}

Example: A public web server with no private information is expressed as:

Security Category(SC)
public information= **{(confidentiality, n/a),**
(integrity, moderate),
(availability, moderate)}.

Evaluation Questions

NIST: Information Security, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

Confidentiality:
How can a malicious adversary use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?

How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?

Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders, or agency regulations?

Integrity:
How can a malicious adversary use the unauthorized modification or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?

Would unauthorized modification/destruction of elements of the information type violate laws, executive orders, or agency regulations?

Availability:
How can a malicious adversary use the disruption of access to or use of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?

Would disruption of access to or use of elements of the information type violate laws, executive orders, or agency regulations?

Information Type Selection

NIST: Information Security, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

NIST places payroll under the Information Type:

Compensation Management

"Compensation Management designs, develops, and implements compensation programs that attract, retain and fairly compensate agency employees. In addition, designs, develops, and implements pay for performance compensation programs to recognize and reward high performance, with both base pay increases and performance bonus payments. This sub-function includes: developing and implementing compensation programs; administering bonus and monetary awards programs; administering pay changes; managing time, attendance, leave and pay; and ***managing payroll****."*

Recommended security level for Payroll Department:

Security Category (SC):

Confidentiality, Low
Integrity, Low
Availability, Low

NIST Discussion and Review of Impact levels

Confidentiality:
"The confidentiality impact level is the effect of unauthorized disclosure of compensation management information on the ability of responsible agencies to design, develop, and implements compensation programs that attract, retain and fairly compensate agency employees will have only a limited adverse effect on agency operations, assets, or individuals."

Special Factors Affecting Confidentiality Impact Determination: *Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974. The 1977 Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. In a few cases (e.g., where some employees are potential targets for retaliation by criminal elements or targets of foreign intelligence organizations), unauthorized disclosure of some compensation management information (e.g., name, address, title, organization, dependents' information) can have life-threatening consequences and has a High confidentiality impact level.*

Integrity:
The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. Compensation management activities are not generally time-critical. Special Factors Affecting Integrity Impact Determination: An accumulation of small changes to data or deletion of small entries can result in excessive disbursements of payroll, bonus and monetary awards or affects pay changes, time and attendance, etc. In some cases, the adverse effects of consequent negative publicity on mission functions or public confidence in the agency can be serious. In some other cases, integrity compromises that adversely affect a significant subset of the workforce can result in staff issues and works top pages that adversely affect the agency's mission. Where interruptions to agency missions can have serious or life-threatening consequences for individuals, the impacts of integrity compromises can be moderator even high.

Availability:
The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to compensation management information. Compensation management processes are generally tolerant of delay. Typically, disruption compensation management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: *The provisional availability impact level recommended compensation management information is low.*

Finalize Impact Levels

The following is the example of information categories and impact for payroll:

Information Type	CIA/AIC Triad Impact		
	Confidentiality	**Integrity**	**Availability**
Employee General Info (Title, email, directory info on a public domain)	Low	Low	Low
Employee Internal Information Governed by Policy (wages, reviews, discliplinary actions, photos, other employee data, timekeeping sheets)	Moderate	Moderate	Low
Employee Confidential Information Governed by Law (social security # and name, bank account information and cardholder name for direct deposit, driver's license and name, health information)	Moderate	Moderate	Low
Employer Bank Account Info for Payroll (accounts used to pay employees)	Moderate	Moderate	Moderate

The above chart classified four main types of data. The top three categorize levels of Employee data and the fourth classifies company bank account information.

Recommended system security level for Payroll Department by CompanyX Team:

Security Category (SC):

Confidentiality, Low-Moderate
Integrity, Low
Availability, Low

Finalize Impact Levels

We can derive the impact levels from brainstorming real world risks:

Security Objective	Impact Examples		
	Low (Limited Adverse Effect)	**Moderate (Serious Adverse Effect)**	**High (Severe or Catastrophic Adverse Effect)**
Confidentiality	Pay rates of workers are witnessed or overheard during discussions with HR or email	HR & Management Login Credential to HR portals leaked due to Phishing/Vishing scam	N/A
	Communication error regarding direct deposit or bank account information	Policy for Anonymous reporting to HR NOT kept anonymous	N/A
Integrity	Buddy punching: coworkers arrange to clock each other in as they take days off	Misonfiguration in cloud portal allows worker to elevate privileges and change pay rates or hours worked	N/A
	Payroll advances not paid back by employee	Ghost Employee: Checks paid out to fake employee(s) draining funds	N/A
Availability	Low intesity DDOS on payroll portal	Mid to High intesity DDOS on Payroll portal	N/A
	Ransomware temporarily freezes records until backups are used	Ransomware Malware wipes out HR records	N/A

Recommended system security level for Payroll Department by CompanyX Team:

Security Category (SC):

Confidentiality, Low-Moderate
Integrity, Low-Moderate
Availability, Low-Moderate

References

Bosworth, S. & Kabay, M.E., & Whyne, E. (2014). *Computer Security Handbook, Sixth Edition. Volume 1.* Hoboken, Ney Jersey: John Wiley & Sons, Inc.

Bragg, S. (2017, May 4). *Types of payroll fraud.* Accountingtools.com. https://www.accountingtools.com/articles/2017/5/4/types-of-payroll-fraud

Deloitte. (2016). *Payroll leakage. What it is and how to fix it.* Deloitte.com. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-payroll-leakage-what-is-it-and-how-to-fix-it.pdf

Ferguson, G. (n.d.). *The Confidentiality of Payroll Information*. Chron.com. Retrieved from http://smallbusiness.chron.com/confidentiality-payroll-information-40356.html

NIST. (2008a, August). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. NIST.gov. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

NIST. (2008b, August). NIST: Information Security, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. NIST.gov. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

NIST. (2017, January 10). *P4038-R Greyhound - Detailed Business Case For Implementing A Human Resource Management System Strategy: Compiled And Presented By EIMS Project Core Team.* Justice.gov. Retrieved from https://www.justice.gov/atr/p4038-r-greyhound-detailed-business-case-implementing-human-resource-management-system-strategy

CSU. (n.d.). *Data Protection*. Csuchico.edu. Retrieved February 2, 2018 from http://www.csuchico.edu/isec/data_protection.shtml