Sheri L. Wilson

Capella University

**TS8535 - System and Application Security Advances**

**December 13, 2023**

**Assignment 10: Leveraged Identity Authentication**

**Table of Contents**

[Executive Summary 3](#_Toc153389162)

[Internet Security: Account Profiles 4](#_Toc153389164)

[Use Cases 4](#_Toc153389165)

[The System and Application Security Issue(s) 5](#_Toc153389166)

[Research Problem 6](#_Toc153389167)

[Limitations of the Study 8](#_Toc153389168)

[Problem Simplification 9](#_Toc153389169)

[Background 10](#_Toc153389170)

[Significance of the Study 12](#_Toc153389171)

[Research Method 15](#_Toc153389172)

[Research Questions 15](#_Toc153389173)

[Data Collection 16](#_Toc153389174)

[Definitions 17](#_Toc153389175)

[Single User Account Data 18](#_Toc153389176)

[Quantitative Research 19](#_Toc153389177)

[Rules, Policy, Regulations, Law 19](#_Toc153389178)

[Conclusion 21](#_Toc153389179)

[Literature Review 21](#_Toc153389180)

Executive Summary

The internet account system has grown, now requiring security on every site that includes personal identity information. It must be secure, so people are now required to create a profile and maintain account credentials. This means a user creates a profile for each Internet Site it interacts with, which can result in a very high number. There are two types of Authentication Methods: 1) Individual User Account (IUA); or 2) Leveraged Identity Account (LIA). Not all sites offer both methods, in fact, most internet sites require users to create a profile and the site maintains personal information and manages site security. Users are responsible for updating the data. LIA’s have recently been introduced that allow users to select an existing account for use as sign in credentials on a new site, which has proven to save much time and reduces the necessity to retype or replicate existing information. The information is maintained in a central location, by the main provider of the chosen account. There are several problems with both methods. It is suspected that the greater number of IUA accounts and LIA accounts, the greater the risk of data loss or breach, and the greater the number of IUAs the greater the management burden. This study aims to prove greater efficiency in the use of LIAs and to show problems with both personal information management solutions. It will include quantitative research for one user and the user experience of a developer when creating a regular e-commerce site and the process for using leveraged accounts. It will include the risks and benefits of both.

Internet Security: Account Profiles

Leveraged Identity Authentication (LIA) is the concept of using security products developed by a third party, accessible using an Application Protocol Interface (API). The use of LIA enables centralized and simplified account creation and management. There are more than three options of LIA that increase the complexity of the management task and each of the three options has different management features. Traditional profile management or privacy data management is Individual User Account (IUA), where each profile is managed individually on every site it provides data. LIA enables a new user to create an account and use a secure site within just a few clicks, which authorizes the new site to use existing account information. The alternative to LIA is IUA, which requires the completion of a new user account, which might require different information in different formats, requiring the management of information on that specific site.

# Use Cases

A client wants a secure E-Commerce Site that handles secure credit card transactions for the exchange of goods and services. It does not want to manage user accounts or be responsible for maintaining user data, but it wants users to be able to securely make purchases from their online store. The recommended solution is the “Sign in With” feature, offering three options. The selected privacy and account management in this study is the “Google One-Tap Sign In” which enables the sharing of secure account information for the transaction. Although it requires more than one tap to register a new account, this method leverages an existing account managed by a primary provider: Google, Inc. Because security is managed by a third party, the individual online retailer lowers its risk and responsibility and users can shop, socialize, and do business online with a lower responsibility of information security management, thus lowering risk and responsibility in two places because of leverage. Google offers a centralized data privacy center that enables users to view and manage accounts in one place through data use authorizations. Other options are to use another LIA, such as Facebook or other social media accounts, or the traditional profile account creation and management system provided by the Internet Site. Information risk, management, and responsibilities change depending upon the method and product chosen.

The System and Application Security Issue(s)

Not all systems offer leveraged account information (LIA). An individually managed duplicative structure is still used, referred to as IUA. Allowing duplication of account information increases variation and is more difficult to manage because information is contained in multiple locations, requiring each location to be accessed to change the same data. It does not follow a relational shared data structure or data entry rules, but data changes and password resets are standardized, but data varies and is stored in many unknown locations. For the user, data breaches are not simple to manage in a non-centralized system, thus requiring edits, changes, and monitoring in many places. This creates inconsistency problems and non-standardization of security practices across the internet, limiting the ability to *efficiently* authenticate and manage computerized accounts and activity. Efficiency measurements must be established. Proof of the theory of causal increase using correlation statistics with a scalable formula for application data management will show greater advantages and lowered risk using the leveraged account information solution compared to the individualized account management system. Does the LIA or IUA follow the Federal Risk Management Framework or do government security standards greatly vary from commercial technology products, processes, rules, and laws?

# Research Problem

Account Management that requires human data duplication requires maintenance in an unknown number of locations with no centralized management system. Account Management and Identity authentication have historically been developed individually for desktop applications that are designed similarly to the Operating System’s authentication procedure, requiring the creation of an account to use the system. The purpose of identity management and ownership of data is for tracking, authentication, and use in multiple areas, such as business, finance, location, and personalization. If a user has multiple security providers, then data cannot effectively and efficiently be brought together by an additional security provider, or one of the providers unless a new solution is created, or a human does it on their own. For example, an Apple user of GPS products has difficulty integrating Google accounts for location and use reports if they use both because the companies do not effectively work together to provide consolidated security or reports. Security is managed in both places, separately by the companies and the users and even more when buying, socializing, or working on other Internet Sites, such as Facebook, or Pinterest.

New privacy control and disclosure mechanisms have recently been developed to help give people who access online applications and services greater power over their personal information and how it is used, as well as to increase transparency and accountability for organizations that collect and process this information (Balash, 2023). This once meant every Internet Site required the creation and maintenance of single account profiles, for each site, with individually managed site security – proven by a small lock image in the browser address bar, implemented by trained security experts and created by new account holders. It was a security structure with roles and responsibilities based on two or more parts: The Company, A Third Party, Sites Security Implementer, and the Account Holder/User. The assumption or understanding was that each technology provider would create or procure a standard security solution, functional in multiple programming languages designed to meet general security requirements of various levels. Although information management is standardized using ‘profile’ and ‘account maintenance’ for each Internet Site and users are willing to create multiple accounts using duplicative manual typing processes to set them up, the industry is lagging in the implementation of an efficient shared data architecture. The more data there is to manage, in multiple locations increases burden, responsibility, necessary storage, and risk.

The problem must be understood from four perspectives: The Security Product Provider, the Developer, Implementer, and the User. All involved parties must also understand the legal responsibility, rules, and ramifications. Since architecture refers to both hardware and software designs, it is necessary to understand both sides of the network operation from more than just one side, therefore it cannot be solved by a simple functional test or product comparison. Test cases and use case scenarios are created to prove the hypotheses, finalized by a summary of product and legal review. A research design and proof must start with an individual user and then be tested with a larger group to prove, even though it can be proven with one single human user who maintains multiple accounts.

Technical challenges exist in separating the technology test cases of data to the analytical review and legal application. Qualitative research is best used for explaining problems related to industry-wide reports and the inability directly apply the law without full explanation of the problem the high number of variations, and locations have caused. First, the problem must be explained, solved, and then the solution recommended, but it first must be compared to other solutions, carefully controlling the scope of the study. The use case is designed to prove efficiency in data and privacy management using Leveraged Account Information (LIA). It is unknown if the use of Google’s Sign in With code feature is reliant or affected by low-quality security of the information site it is used on, or if security functionality and risk are transferred. It is also unknown what information is transferred and stored in Google, Inc.’s possession, maintained in their system and for how long, thus transfer of risk and data responsibility remains only a partially understood and partially managed problem. “All of our products are guided by three important principles: With one of the world’s most advanced security infrastructures, our products are secure by default. We strictly uphold responsible data practices so every product we build is private by design. And we create easy-to-use privacy and security settings so you’re in control.” (Pichai, Google I/O 2021).

# Limitations of the Study

One of the important limitations of the study is that it can only be tested as a user and not as an information security network manager of leveraged account development and management because it requires the use of third-party technology or another account, where insight is limited. In a limited capacity, it can prove ease of use for developers using LIA Products via an API as a recommended security solution, but to reduce complexity, LIA and API must be both generally explained and studied in detail to prove the theory that lower number of accounts in central locations (or the reuse of existing data) results in lower risk that simplifies the complex ‘risk management’ design created by previous security assessors.

Since the success of Internet Applications and Mobile Technologies, security protocols have been standardized and followed, requiring identity authentication for every Internet application, with additional and separate security for networks, internet connectivity, and now merchant accounts, as well as other popular Internet applications categorized as social media and now even account management for interactive internet sites. Security breaches, including data hacking, monetary and identity theft, and social engineering, continue to be reported to be on the rise. How does this affect the LIA solution? Bad information regarding security, including scare tactics, fear and risk-based approaches, as well as a large set of unknowns has the potential to affect the results, as well as the selected solution. Because of the invention and popularity of “Artificial Intelligence” and “Information Assurance,” the necessity for real authenticated data in online transactions is critical, but so is centralized user-managed data security. Sharing of data amongst service providers, commerce, and social systems is considered the most efficient, which is why technologists are now willing to work together to leverage what used to be individually developed ‘code’ for account management creation and security. Not all e-commerce and online profile systems leverage existing account authentication and management methods, which causes more work and variation that seems like it cannot be statistically evaluated because of the vastness of the Internet and the high number of business and social transactions or sites that are managed by account.

# Problem Simplification

A security architecture of interconnectedness that leverages secure account management is vital, which requires a change to more than just a security policy, awareness, press releases or media, technical code, database management, threat-based monitoring, and developer choice. It is as simple as a task for a developer to choose whether to use existing code from a trusted provider, such as Google, Inc., or Facebook that allows users to leverage account information, alleviating them from the task of creating another one to manage, or to use its own account management system, in which it is responsible for the protection of personal data and has access to because it stores it. There are unknowns, which impact security. It is unknown if using Google’s security functionality by adding code or connecting through an API is dependent upon the internet site that the code runs on and to what extent. Because of customization, it is also unknown what data is shared and where. It is minimally explained to users that they are authorizing a third party to provide sign-in credentials and personal information to create a profile or to complete transactions on the new site. It is also not clear where those authorizations are managed.

Re-clarification of the scope of security must also be explained and correctly applied to the correct management system. Rather than teaching users how to create secure accounts for each merchant or internet site, and using awareness to instill user responsibility, a change to security processes from one side is required, with implementation across the Internet to change how Internet Sites (and possibly more) are created and managed. The fruit of the poisonous tree and virality must be considered, as well as a theory of Complexity. The result guarantees a benefit that can be seen as a change to the improper transfer and balance of risk and responsibility. Currently, security risks are spread out and by bringing them together, they can then begin to be defined and effectively managed, but first risk must be separated from trust, and roles and responsibilities must be well understood, standardized, and proof of improvement to even begin a system security evaluation from a two-part perspective. The “generalization” and references to “application security” must become more detailed in terms that users understand, as does a division of responsibility. Efforts to automate must also be established, separating redundant manual and cumbersome tasks from those that are more secure and automated and what it means in terms of management, risk, and change.

# Background

Security awareness is an educational endeavor, and by doing this, security risk has been transferred to the users, with developers and site owners assuming people can and should manage device and application security on multiple levels, in multiple places, and with many different companies, processes, and details of promise or service. This has created a security problem that raises the question of whether there is a better architecture or some solution that could centralize and standardize security. Are humans misled to believe security is not their responsibility or that they do not have enough information to adequately manage security, and can technology be more effective in its security process? The main problem is internet shopping, socializing, and doing business which has resulted in a high number of accounts, and is unnecessarily duplicative, which is hypothesized to increase error and time, increasing the rate of problems, resulting in future mismanagement and possible misfortune. This is expected to become an even greater problem as humans age. It has also resulted in bad publicity in the security sector and lowered consumer confidence, of which there does not seem to be a standard protocol or study available for how these critical problems are measured and solved.

Risk and crime are not the only problems, even though they are major. Because of the freedom the internet offers and because of automation, the botnets and hackers have creatively engaged in regular criminal activity online, including cyber-bullying, and theft, and have extended into fake intelligence or the creation and spread of false information, all proving to cause significant damage to people and businesses across the world. Individual training and awareness placed a burden on every user. Fake media is also on the rise, leaving consumers fearful, yet communicative and somewhat knowledgeable about what is happening in computer security.

The idea of creating a single security suite to manage security profiles that can organize all critical information in a centralized location is viewed as a great risk if compromised or misused, thus several efforts, such as individual security accounts with manual organization, multi-factor authentication, and some cyber security practices have been implemented. The theory is that if everything is in one place, then everything can be quickly compromised, causing greater damage and the alternate theory is that if everything is maintained using one security profile, then simplification increases security because of the lower number of places to manage necessary change for multiple events, enabling faster resolution and improved management by one trusted company and user. The multiple events are changes to personal details, emergency account changes, accessibility, and other information management tasks. Centralized security is of great benefit for efficiency and information management purposes if it is secure and reduces the risk of theft or misuse. It is also hypothesized that an increase in the variation of security options adds to the conceptual risk profile because of individualized approaches which becomes an unmanageable problem. Although risk is often spoken of, it is believed that if there are individualized non-standard security approaches to application account management, then there are also non-standardized risk assessment procedures, making security appear to be professionally management, with varied informal and inconsistent processes, which is what a disorganized criminal or a member of organized crime benefits from. Complexity and decentralization make it more difficult to manage. Users (the people) should have a standard risk assessment process, along with a standard security process, but they do not; it is up to each individual to use the correct setting, select the right solution, and securely manage the information.

There are two problems to solve: the data architecture and user management, which both have direct causal relations to economics, crime, and longevity. Because of the long list of benefits of a centralized system, it must be carefully examined before investment. If developers continue to create varied security solutions, then they cannot solve existing problems, so a stop-work process must be created and placed on all development resources across the world since it poses the greatest risk. If people and management don’t view it as a problem, then work continues as usual until the problem is formally presented and proven to cause or increase risk or reduce complexity and meet efficiency criteria for improved use.

# Significance of the Study

Establishing software product efficiency criteria can be an adopted standard applied to all software, not just security. Specific risk criteria and benefits can also be applied for consideration of other products. The metrics used to evaluate software enable informed selection, which improves user and/or consumer confidence. The study can be applied to other software systems to show where efficiencies can be gained by using a leveraged approach to functionality. The significance of the sharing of personal data has been overcome and has become a complex profitable field for security experts, therefore ethics and economics are of great importance. If industry continues to create varied and more complex systems, it just replicates and continues the problem of allowing information to be secured in many different places. The same is true if virtual security is governed by state law by using a physical enforcement system.

Reviewing the number and functionality variations of security products is a heavy task, as is understanding and explaining overall security problems with the current process when viewing the entire internet user population, or many layers of security so the study is limited to just the account management function. To manage the scope of the project, a developer single-user study is presented. Before the research model can be applied to others, levels of experience must also be gathered and evaluated. Without empirical data to show the effectiveness of such practices, efforts continue to strengthen the security system of the Internet as it expands access to other devices including mobile and the development of the Internet of Things. It remains a generalized problem, using threat-based concepts, where breaches and hackers are the number one item for report in CyberSecurity News, when positive reports could show the improved structure gained through interoperability or sharing of data. As the Internet grows, risk grows, as do security problems, and the industry adapts through changes like improved security practices in code development, the use of biometrics, online security awareness, and new approaches such as the Federated Identity Model and leveraged Authentication. If the number of accounts grows and increases security risk and results in mismanagement and can be proven, then it can also be believed that as the number of security options and variations grow, the risk also increases to a point of unmanageability and terms or processes can no longer support the design, therefore it must evolve. The “Risk Management Framework” requires reconsideration of the ways in which security is viewed to look beyond a single application and single user view into much higher numbers to understand, prove, and accept the theory. The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations (NIST, RMF, 2023).

There is a greater focus now on user experience, with much effort and attention on security. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled (Barton, et. al, 2019). Even though organizations implement and follow strong security standards and the ISO 27000 Series has ***60 standards*** covering a broad spectrum of information security issues (Kirvan & Granamann, 2023), few engineers have concluded that the security architecture is not the best fit for advanced cyber-evolution and have only slowly taken on an integrated and centralized approach to security. To effectively convey the security problem, it is necessary to understand the burden and risk placed on its users, with better efforts to engineer a solution that solves the problem. Rather than transfer risk and responsibility to the user with varied complexities in many locations and expecting security procedures to be learned and followed by every security company, developer, and user, it's lower risk to centralize the design. Because of the uniqueness and critical necessity for personal data, as well as its frequent use, it's important to have the most effective system, and not a department store of options. The research study must follow the quantitative scientific research method to prove its theory, this means the theory must be defined, with double hypothesis testing using the standard method of statistical analysis.

# Research Method

The study will use quantitative research and statistical analysis to compare the average number of online accounts per user, number of leveraged accounts, number of individual accounts and necessary management time. It must also review a small sample of password reset frequency, along comparison of the two security products. It will reference existing broad published research on security breaches for online accounts and processes for small organizations to monitor or evaluate security policies. The research must also note that if industry continues to create more security solutions, it counter acts the study’s efforts in proving the fewer amount of data to manage, the lower the risk. More variables may be added. It will create a risk and efficiency scale and compare the two methods. It will also show how responsibility changes, transferring risk, which becomes unmanageable and unknown and will prove problematic in data management or increased burden placed on uneducated users.

# Research Questions

What is more efficient and simplified: LIA or IUA? Is it of lower risk and benefit for a centralized account management system with a more organized and integrated authentication system? Which side of the two- or three-part of security responsibility benefits most? Of the total number of accounts, how many leverage existing accounts and is it easily managed using a centralized system? How is the Risk Management Framework applied or changed by choosing a different method? Is offering multiple security options adding more complication to security management and what is the most professional security strategy for new and existing accounts? What are both security processes and why is one better than the other? Is a single-user research study sufficient to create efficiency and risk standards to change the current security practice industry-wide, or do other solutions need to be evaluated for product comparison? If limiting developers and companies using standards is a violation of free commerce, one must consider America’s backbone as Economics and treat personal data of great value and a matter of National Security, to not only enable the use of technology systems, but to efficiently manage and protect for more than just economic security, but also use by more than just users of data, but owners, and other interested parties. It is hypothesized that the data will show a greater amount of time is required to manage IUAs in comparison to LIAs, that security awareness strategies are outdated, that a new risk management strategy is required, and that one company is better than another in terms of LIA management from both a developer’s perspective and user perspective.

# Data Collection

Data will be collected to compare time savings between leveraged user accounts and individual accounts. It will attempt to show how decentralized account management using a 1:1 ratio is dangerous, proving that the more data there is to manage, the greater the risk of harm. Statistical analysis of the data collected will show time and process variations for both methods and will present comparative risk management metrics. A second data collection phase might be conducted using survey data from random participants in a small community, as well as random online participants. The questions will be designed following the quantitative research standards model of survey questionnaires, adhering to ethics to obtain quantitative data. Confidentiality is important and ensuring safe handling of information and protection of personal data. Specific informed consent will not be necessary because it is only a one user sample, with a model that can be scaled for other users.

# Definitions

 Individual User Account: An individual user account is a single profile completed on an internet site or internet site application where a username and password are required, along with personal profile details. These are managed site by site. It is a similar, but not exactly the same standard login process for each site and requires users to ‘retype’ the same profile information, and allows variation in username, passwords, and personal information.

 Leveraged User Account: A leveraged user account uses an existing account, such as Google, Facebook, or AppleId to manage its personal account information. It uses a management console that enables users to control access to other merchants or providers of Internet goods and services. It is a three or four-step login process with no typing required.

 Risk Management Terms: Acceptance, Avoidance, Transfer, Mitigation. These are terms used in the Risk Management Framework for Security of Applications. Risk is considered accepted by the users when setting up a profile, and risk is considered transferred by the Technology community, along with information management responsibility. Risk increases when data mismanagement opportunities and inconsistency exist. Perceived risk is a non-proven risk of trusting only one company or application with personal privacy data management. Risk is considered mitigated by users who utilize a centralized password vault, paper process, or third-party application to manage multiple security profiles used in many places. Risk terms from a developer perspective is also transferred to the provider of security application code implementation using LIA and risk responsibility are uncommunicated mitigation actions completed by security product providers, and data users which encompasses more than a single person, including those who require, use, share, sell, and store the personal data. Risk responsibility is critical to clarify roles and actions required to change media alerts, and viral scare tactics, and to manage security efforts properly for more than just the consumer/user.

# Single User Account Data

The table below will be used to collect data to summarize and statistically present once the data has been collected and analyzed using JASP, a statistics calculator. Process comparisons of LIA and IAM will also be presented in the dissertation project.

|  |  |
| --- | --- |
| **Individual vs. Leveraged Accounts** |   |
| Total Number of Individual Accounts |   |
| Profile Setup Time/Steps |   |
| Login Time/Steps |   |
| Reset Time/Steps |   |
|   |   |
| Total Number of Leveraged Accounts |   |
| Profile Setup Time/Steps |   |
| Login Time/Steps |   |
| Reset Time/Steps |   |
|   |   |
| **Data Analysis** |   |
| What is the average amount of time spent on Profile Setup |   |
| What is the total average login time for Individual Profiles |   |
| What is the total average login time for Leveraged Accounts |   |
| What is the total average time for Personal Detail Change Leveraged |   |
|   |   |
| The difference between the averages |   |
| Number of possible variations of account information |   |
| Number of actual variations of account information - leveraged |   |
|   |   |
| **Account Management Console** |   |
| Leveraged Google Accounts | 36 |
| Individual Accounts (managed by Human Memory) |   |
|   |   |
| **Newsletter Subscription Management** |   |
| Individual |   |
| Managed by Google |   |
| Total Number of Subscriptions |   |
|   |   |

# Quantitative Research

Depending upon the quality of data and meeting the goals and objectives of single user study of data privacy account management methods. It must prove a greater than risk theory using a decentralized manual process or human memory and low quality internet browser system for account management, proving need and opportunity for a secure integrated account management system.

# ****Rules, Policy, Regulations, Law****

The Privacy Act of 1974 establishes **a code of fair information practices** that govern the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies (Privacy Act of 1974, 5 U.S.C. § 552a, 1974). The Freedom of Information Act applies only to federal agencies and not to records held by Congress, the courts, or state or local government agencies. Each state has its own public access laws (The Freedom of Information Act, 5 U.S.C. § 552). The Digital Millennium Copyright Act is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization, criminalizing the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (Digital Millennium Copyright Act, Pub. L. No. 105-304,1998).

The availability of information, from personal information to public information, is made all the easier today due to technological changes in computers, digitized networks, internet access, and the creation of new information products. The E-Government Act of 2002 recognized that these advances also have important ramifications for the protection of personal information contained in government records and systems (DOJ, 2019). Privacy Impact Assessments (PIAs) are required for Federal Agencies that develop or procure new information technology involving collection, maintenance, and dissemination of information in identifiable form or that makes substantial changes to an existing system (E-Government Act of 2002, Pub. L. No. 107-347, 2002). Local and state laws vary regarding rules of use of personal information; the state of Virginia prohibits the processing of sensitive data without obtaining consumer consent (Va. Code § 59.1-578). The processing of sensitive data also triggers the obligation to conduct and document a data protection assessment (Va. Code § 59.1-580). The state of California’s Consumer Protection law is much more specific in delineating consumer rights of personal information protection (CA DOJ, CCPA, 2023). The Virginia Consumer Data Protection Act (VCDPA) clearly defines whose personal data is covered, describing consumers as Virginia residents “acting only in an individual or household context.” It further clarifies that consumers are not those acting in a “commercial or employment context.” Unlike California, where the now-expired B2B and employee exclusions have been the subject of several statutory amendments, Virginia has chosen not to leave those potential compliance hurdles up in the air (Bloomberg Law, 2023).

If specific laws that govern the protection of personal information are state by state, then another problem exists in security protections, as are the procedures for remedy when the laws are violated. Therefore, the responsibility for the security of personal information must be clarified and added to the argument that a single provider of security products for consumer use is beneficial for more than just efficiency, but legal purposes.

#

# Conclusion

 The Internet has been around for nearly 40 years or more, now used by the public to perform daily work functions and social exchange. Because identity and financial or personal information has always been something unique that requires protection, the security industry has done its best to provide secure systems to shop, socialize, and perform regular life functions. In its growth, security has adapted to the changes, using an individualized approach, securing network connections, and site-based connections. It has not offered advanced management solutions for the information that is protected, and the software systems owners carry some risk and responsibility for the management of data, during and after transacting. The risk has transferred onto the users, with site owners guaranteeing security and no one really evaluating the architecture for a more efficient design. They’ve accepted the design as is an account for each secure internet site, a 1:1 ratio when a more relational or integrated architecture or design is possible. We’re only now seeing opportunities to leverage code, follow authentication standards, and offer centralized management solutions that are written with clear instructions, but much is missing. There is a more efficient and effective design that is guaranteed to reduce risk.

# Literature Review

1. Federated Identity is a service provided by a **third party that enables participating organizations to leverage home organizations' digital identities**to**access partner resources**by implementing a**common standard for technical interoperation.**

Barton, et. al, (2019), 7 Things You Should Know About Federated Identity, EDUCAUSE
Publications accessed via the Internet at https://library.educause.edu/resources/2019/1/7-
things-you-should-know-about-federated-identity

Informative Article

1. If technology can help bridge the design gaps we have, and perform tasks that are mind-numbingly repetitive, why not let it? This article discusses the human condition and evolution with technological assistance.

Kandala, K. (2018), Digital Paranoia: Modern Form of Existential Crisis, accessed via the
Internet at https://medium.com/swlh/digital-paranoia-a-case-of-existential-crisis-
d2a53ec977c1 on October 17, 2023

Informative Article

1. This is where IT security frameworks and standards are helpful. Knowledge of regulations, standards, and frameworks are essential for all infosec and cybersecurity professionals. Compliance with these frameworks and standards is important from an audit perspective, too.

Kirvan, P. & Granneman, J., (2023), Top 10 IT security frameworks and standards explained

*Tech Targets,* accessed via the Internet at https://www.techtarget.com/searchsecurity/tip/IT-
security-frameworks-and-standards-Choosing-the-right-one on October 17, 2023

Informative Article

1. There is an assumption based upon brand recognition that a user’s sense of security correlates with their knowledge of the popularity and success of technology business names. This is a study about brand recognition theory using psychology methods, attempting to apply it to Big Technology names and user’s perception of security and trust in software.

 The Role of Big Tech in Providing Cybersecurity to End Users: A Qualitative Case Study,
Morgan, J.M (2023), Northcentral School of Business, San Diego

Methodology: Qualitative Case Study

1. The Digital Forensics Framework, which is still in its infancy, makes the requirement for hybrid solutions, and creates a conflict or proves delay between law enforcement and technology, increasing security risk.

 Quick, Martini, B., Choo, K.-K. R., & Shavers, B. (2014). Cloud storage forensics (1st edition). Elsevier.

1. Copyright and intellectual laws, along with privacy and legal issues as it relates to cloud computing is reviewed. There is no specific “theory” used to articulate the challenges, nor does it suggest how moving to the cloud reduces risk or changes laws. Ownership of data, sharing and other legal issues are still possible, and potentially even greater due to an open programming model that enables a wide variety of security options at the discretion, and control of businesses, and users.

 Cheung, A. S. Y., & Weber, R. H. (Eds.). (2015). Privacy and legal issues in cloud computing. Edward Elgar Publishing Limited.

1. Consumer Privacy Legislation by State; privacy-related laws; how do they stay current with cloud computing evolution? Consumer protection acts and do not sell my information remains on the forefront, as does state by state legislation issues with jurisdictional boundaries often crossed in dealing with E-Commerce and information transactions, increasing the need for digital forensics. Consumer awareness studies and a framework for empirical data reviews are also missing.

 2022 Consumer Privacy Legislation, National Conference of State Legislature, accessed via the Internet at https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation on Oct 30, 2023

1. Cognitive Information Processing Theory as it relates to career and adult development. A well-known theory applied to human development not correlated to security systems, or medical device tracking. I attempted to find a study that related the human design of psychology as it correlates with computer processing in information management, with overlaps in terminology, but was unable to find anything.

 Osborn, D. S., Hayden, S. C. W., & Brown, C. (2020). Chapter 1: Cognitive Information Processing Theory: International Applications. Career Planning and Adult Development Journal, 35(4), 4-16. Http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Ftrade-journals%2Fchapter-1-cognitive-information-processing-theory%2Fdocview%2F2573517889%2Fse-2%3Faccountid%3D27965

Scholarly Journal

1. Wearable in ear device for Electroencephalography Based System for Biometric Authentication. EEG’s brain wave scan ability for use as security biometrics, suggesting brain scan devices worn in the ears can be used for biometric authentication.

 Hwidi, J. (2023). *Wearable In-Ear Electroencephalography Based System for Biometric Authentication*(Order No. 30770766). Available from ProQuest Dissertations & Theses Global. (2873028071). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fwearable-ear-electroencephalography-based-system%2Fdocview%2F2873028071%2Fse-2%3Faccountid%3D27965

Dissertation, Quantitative Study

1. Direct Brain to Device Connections, review of documented technology and possible security problems and solutions. Advanced authentication, perhaps the best form of biometrics, and additional knowledge management functionality, it appears solutions are added to the long list of possible authentication methods, going from brain scan to wearable technologies, when the technology itself requires a standard authentication method, integrated with other systems, but with possible sensor technology.

 Ortega, A. (2023). *Wearable Brain Computer Interfaces with Near Infrared Spectroscopy*(Order No. 30242215). Available from ProQuest Dissertations & Theses Global. (2769193628). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fwearable-brain-computer-interfaces-with-near%2Fdocview%2F2769193628%2Fse-2%3Faccountid%3D27965

Dissertation, Qualitative Study

1. Relationship between Self-Identity Confusion and Internet Addiction among College Students: The Mediating Effects of Psychological Inflexibility and Experiential Avoidance. Are there any related studies or field research on the correlation of technology identity and personal identity problems, and solutions? Identity authentication is varied in computer systems, offering several options, left at company or developer discretion, requiring a high number (non-quantified) and duplicative tasks, proving a non-integrated authentication architecture in Internet or Cloud Systems.

 Hsieh, K. Y., Hsiao, R. C., Yang, Y. H., Lee, K. H., & Yen, C. F. (2019). Relationship between Self-Identity Confusion and Internet Addiction among College Students: The Mediating Effects of Psychological Inflexibility and Experiential Avoidance. International journal of environmental research and public health, 16(17), 3225. https://doi.org/10.3390/ijerph16173225

Scholarly Journal

1. Your Head is in the Clouds is an old saying. Since Cloud Computing is new, research is required on using brain imaging technology and cloud computing systems beyond medical information, as well as a higher level of security. It’s necessary to review the similarities published by the American Psychological Association to what is being done, said, and referred to in Technology.

 How to Keep Your Head in the Clouds: Cloud computing concepts are giving developers freedom and flexibility in application deployments. (2009). *Information Management, 19*(3), 18. http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fhow-keep-your-head-clouds%2Fdocview%2F214668988%2Fse-2%3Faccountid%3D27965

Scholarly Journal

1. Half A Century In CT: How Computed Tomography Has Evolved. The CT-Scan has evolved with the introduction of cloud computing. Medical imaging and radiation therapy professionals need more education in CT technology, including potential laser therapies, and research into information transfer in both digital and physical matter; a combined physics and computer science endeavor would advance the technology, but requires a controlled test in confined spaces.

 Half A Century In CT: How Computed Tomography Has Evolved, International Society for Computer Tomography, CT Evolution, Oct 2016 accessed via the Internet at https://www.isct.org/computed-tomography-blog/2017/2/10/half-a-century-in-ct-how-computed-tomography-has-evolved#:~:text=In%201967%20Sir%20Godfrey%20Hounsfield,Laboratories%20using%20x%2Dray%20technology.&text=In%201971%20the%20first%20patient,publicized%20until%20a%20year%20later. On Oct 30, 2023

Methodology: Qualitative Informative Study

1. Security Awareness Studies on Single Sign-On Solutions of Students

Pratama AR, Firmansyah FM, Rahma F. Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. PeerJ Comput Sci. 2022 Mar 11;8:e918. doi: 10.7717/peerj-cs.918. PMID: 35494842; PMCID: PMC9044249.

Methodology: Quantitative Research

1. User Behaviors and Attitudes towards password expiration policies.

Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies. Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, pp. 13-20.

Methodology: Quantitative Analysis of Survey Research

1. Diversifying Passwords to Survive: A two-part online study to examine how participants create and use passwords under two adaptive password policies in multiple configurations.

 Sean Segreti, William Melicher, Saranga Komanduri, Darya Melicher, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Cranor, and Michelle Mazurek. Diversify to Survive: Making Passwords Stronger with Adaptive Policies. SOUPS 2017, Santa Clara, CA, July 12-14, 2017.

Methodology: Quantitative Analysis of Survey Research

1. According to Verizon’s 2022 Data Breaches Investigations Report, 82% of data breaches involve a human element. In today’s volatile cyberattack landscape, every business in every industry is at risk of a cyberattack. That means that every business needs to make sure that it’s taking a strong defensive posture with the right solutions in place to reduce risk. One of those solutions should be a robust security awareness training program.

ID Agent: These 10 Facts About the Benefits of Security Awareness Training Are Game-Changers accessed via the Internet at https://www.idagent.com/blog/10-facts-about-the-benefits-of-security-awareness-training/

Article Review of Verizon Study Methodology: Quantitative Survey

1. Cybercriminals were quick to exploit vulnerabilities. Organizations reported a dramatic increase in malware attacks. The 2020 FBI Internet Crime Report collated data from 791,790 complaints -- a jump of more than 300,000 from the prior year. These victims claimed losses of more than $4.2 billion.

 Tech Target, DeCarlo, A., What are the elements of modern network security architecture, July 2023 accessed via the Internet at https://www.techtarget.com/searchnetworking/tip/What-are-the-elements-of-modern-network-security-architecture

Article of Quantitative Study

1. This generic qualitative study explored the factors that influence the state of information security governance in modern non-IT organizations across North America. The study was framed within the general deterrence theory and used two research questions as a guide. The first research question was what factors influence the effectiveness of ISG policies in non-IT organizations? The second research question was what strategies do non-IT organizations employ to enforce policy compliance?

 Kamaziwe, D. W. (2023). *Information Security Governance Shortfalls in Non-IT Organizations: A Generic Qualitative Inquiry*(Order No. 30494236). Available from Dissertations & Theses @ Capella University. (2818503049). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Finformation-security-governance-shortfalls-non%2Fdocview%2F2818503049%2Fse-2%3Faccountid%3D27965

Capella Dissertation: Qualitative Study

1. This study focused on cybersecurity risk management for the residential real estate industry. The residential real estate industry is an ongoing target for hackers given its information-rich transactional data. The study research question was Which cybersecurity risk management policies do experts in real estate cybersecurity recommend that managers of residential real estate firms implement to prevent, detect, and respond to cybersecurity threats, vulnerabilities, and attacks?

 Middleton, T. T. (2022). *Effective Cybersecurity Risk Management Policies for the Residential Real Estate Industry*(Order No. 29261271). Available from Dissertations & Theses @ Capella University. (2694989069). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Feffective-cybersecurity-risk-management-policies%2Fdocview%2F2694989069%2Fse-2%3Faccountid%3D27965

Generic Qualitative Study

1. The usability and effectiveness of the new privacy control and disclosure mechanisms do not always align with expectations and in this dissertation, we identify and address the shortcomings of these mechanisms to enhance their performance and improve their outcomes.

Balash, D. G. (2023). *Usability of Privacy Control and Disclosure Mechanisms*(Order No. 30316226). Available from ProQuest Dissertations & Theses Global. (2792832069). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fusability-privacy-control-disclosure-mechanisms%2Fdocview%2F2792832069%2Fse-2%3Faccountid%3D27965

George Washington University Dissertation: Qualitative Study

1. The Privacy Act of 1974 is a federal statute; a code of fair information practices that governs collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. It is defined as a system or group of records under the control retrieved from an agency regarding an individual.

Privacy Act of 1974, as amended, 5 U.S.C. § 552a, accessed via the Internet at https://www.justice.gov/opcl/privacy-act-1974

Professional Review of Legal Statute

1. The Freedom of Information Act covers public access rights to information records from any federal agency. Not all agencies follow the same procedure for fulfillment of an FOIA, in fact, the term: records have even been defined to conform to this law in what agencies can provide upon formal request.

The Freedom of Information Act, 5 U.S.C. § 552, Department of Justice, accessed via the Internet at https://www.justice.gov/oip/freedom-information-act-5-usc-552

Federal Legal Statute

1. Since digital technology could allow for infinite numbers of exact copies of works to be made, the lawmakers agreed they had to extend copyright to include limits on devices and services that could be used for anti-circumvention in addition to acts of anti-circumvention. In establishing this, the lawmakers also recognized this would have a negative impact on fair use without exceptions, with electronic works potentially falling into the public domain but still locked beyond anti-circumvention measures, but they also needed to balance the rights of copyright holders. The DMCA as passed contained some basic fair use allowances such as for limited reverse engineering and for security research.

Digital Millennium Copyright Act, Pub. L. No. 105-304,1998, accessed via the Internet at https://www.copyright.gov/legislation/dmca.pdf on November 29, 2023

Federal Legal Statute

1. The California Consumer Privacy Act (CCPA) is a state law that covers consumers' protection rights to information, as well as their ability to limit change and gain access to notices explaining privacy practices. Some search engines require a Privacy Act disclosure statement on internet sites to produce an error-free internet search engine scan, but contents vary by state because of state law variation. Compliance checks and automation might be possible but does not exist for all or small internet site developers.

State of California Department of Justice, California Consumer Privacy Act (CCPA), Attorney General’s Office, California Civil Code § 1798.192 (2022) accessed via the Internet at https://oag.ca.gov/privacy/ccpa on November 28, 2023

Legal Statute: California Civil Code

1. Department of Justice, eGovernment Act of 2022 enacts the establishment of Personal Information Assessments (PIAs) for all government agencies and that the PIAs must be made publicly available upon request, unless it is considered a matter of national security.

EGovernment Privacy Information Assessments, Office of Privacy and Civil Liberties, Department of Justice, Feb 2019 accessed via the Internet at https://www.justice.gov/opcl/e-government-act-2002 on November 28, 2023

Federal Statute, Department of Justice

1. The Code of Virginia on Personal Data Assessments, responsibilities of the Controller and protection of the processing and sale of personal information.

VA code § 59.1-575, Ch. 53, Jan 2023, accessed via the Internet at https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ on November 29, 2023

28. Bloomberg Law’s Legal Interpretation of the Virginian Consumer Data Protection Act.

Virginia Consumer Data Protection Act (VCDPA): Everything you need to know about Virginia’s new comprehensive data privacy law, Bloomberg Law, accessed via the Internet at https://pro.bloomberglaw.com/brief/virginia-consumer-data-protection-act-vcdpa/ on November 28, 2023
Professional Law Review

1. Google’s Safety and Privacy Promise; Google’s Product Guiding Principles: 1) Secure Product by Default; 2) Responsible Data Practices; 3) Easy to Use Privacy and Security Settings “so you’re in control.”

Google, Safety Center, Privacy and Security, Pichai, S., 2023 accessed via the Internet at https://safety.google/security-privacy/ on November 29, 2023

Corporate Product Suite Guarantee

1. The Risk Management Framework: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor. Not all security efforts match the Risk Framework; small developments using leveraged Code use different processes but are similar to the RMF. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels.

National Institute of Standards Technology (NIST), Risk Management Framework (RMF), Nov 2023, accessed via the Internet at https://csrc.nist.gov/projects/risk-management/about-rmf on November 29, 2023

US Department of Commerce, Federal Guideline

1. Project Management Methodology and Project Success

A correlation study using statistical analysis to see if project methodology related to project success, with selected demographics, using surveys as the measurement. This study investigated the relationship between project management methodology and reported project success, as well as the moderating variables of industry and project manager experience. The sample included North American project managers with five years’ experience, 25 years of age or older, and experience with multiple project management methodologies. Results: Results indicated that project management methodology has a weak correlation with reported project success, and this correlation is not moderated by industry or project manager experience.

Can project success be considered a non-biased variable to be measured and studied if project managers self-report, are biased on performance or monetarily based projects? If there are no set standardized measurements for ‘project success’ then how can one project be compared to another, similarly, if methodologies differ and are mixed, varied and changeable, or fluid in application throughout a project, how can one or more be solely correlated to project success. It’s a simple rejected hypothesis in all cases because project success has a varied, and non-standardized definition, while some call success “completion,” while others see project success as steppingstones leading to larger acquisitions or ventures, or simply a meeting on scheduled dates, on a specific budget. The difference between failure in success in project management is not based on specific data variables, unless determined in the beginning, without connection to the future, outcomes, and performance checks of an ‘empirical nature’ that extend beyond customer satisfaction, into long term equitable and profitable or severe positive economic and social impact, with political measurements and evaluations, depending upon the level of impact.

Pace, M. (2019). A correlational study on project management methodology and project success. Journal of Engineering, Project, and Production Management, 9(2), 56-65. https://doi.org/10.2478/jeppm-2019-0007

1. Project Study Complexity

The study used a three-stage methodology leveraging the existing Project Management Institute (PMI) framework to define variables and then tested the methodology using case data generated from projects adopting a grounded theory approach. A set-theoretic, multi-value qualitative comparative analysis (QCA) tool helped appropriately configure this empirical case data, and a subsequent Boolean minimization technique then identified the distinguishing factor(s) that explained superior project schedule performance.

This is a perfect example of an attempt by the Construction Industry to use scientific methods, noting PMI Knowledge areas as applicable in determining scientific ‘technologically formatted’ data types, without answering fundamental questions using science. Identify new or unused knowledge areas noted in PMBOK are simple studies using surveys as defined by PMBOK and measuring results to show correlation or understanding and employment or use of knowledge areas in specific projects. It assumes all construction project managers use PMBOK and that their employees or managers understand the knowledge areas: a testable hypothesis, but the study was incorrectly designed to answer it, proving creative writing and inability to apply scientific testing to a merged field of PM and CPM.

Iyer, K. C., & Banerjee, P. S. (2019). Identifying New Knowledge Areas to Strengthen the Project Management Institute (PMI) Framework.*Organization, Technology & Management in Construction, 11*(1), 1892-1903. <https://doi.org/10.2478/otmcj-2018-0014>

1. Four Stages of Making Project Management Flexible

While it sounds nice to attempt to suggest or instill flexibility in stages, it is just not a linear progressive numerical function, nor is it a sequential act of four variables or concepts. The ideals of flexibility are personality and management traits, negotiation fundamentals, and human abilities, or mathematical degrees applied to schedule dates. Flexibility is also related to physical components in biological safety. This ‘scholarly’ article cites BMGT8432’s associated textbook; “Cooke-Davies et al. (2008) argue that a paradigm shift away from conventional project management is required to enable the management of current challenges.” This suggest that some linkage has been performed to either promote the associated text or to sway learners from following specific methodologies, by suggesting ‘flexibility’ and ‘some odd insight’ is required to changing or work with effective project management, although there is no direct evidence. It chooses to use the word “enable the management of current challenges” suggesting a change from conventional methods is required to deal with current methods, circling back to project management traits in general, non-specific terms to succinctly describe the problem; an effective tactic of wasting time and making excuses as to why projects are not completed on time, effectively, to specification, and successful, and then suggesting modernization of management principles are required, with no new information that has not already been introduced by many others in ‘non-scientific’ terms.

Afshin, J. S., Bosch-Rekveldt, M., & Hertogh, M. (2020). The four stages of making project management flexible are insight, importance, implementation and improvement. Organization, Technology & Management in Construction, 12(1), 2117-2136. https://doi.org/10.2478/otmcj-2020-0008

1. A Former Project Manager’s Review of the Internet’s Design – 10 Years Post Implementation

A short book on computerized account process and review of conflicts in industry practices of database-driven software and its lack in account management. It shows a complicated security architecture, simplified for users of the Internet, which functions as patterned data entry for non-businesspeople, managing their own security, with an opportunity to create a better architecture. Alarmingly, the people using computerized systems are not aware of the problem, and computer scientists and technology companies do not see the opportunity to create an integrated system. Part of project management is identifying problems and opportunities, even if out of scope.

*Internet Systems Symptoms and Diagnosis. (2023).* Wilson, S., Independently Published, Savvy Smart Solutions, LLC

1. Project Management Body of Knowledge (PMBOK)

This comprehensive guide contains all the necessary knowledge to obtain the Project Management Institute (PMI) Certification. There are few longitudinal empirical studies on project success, use of the PMBOK, certifications and employment rates. There are also few studies on project failure rates in relational correlation statistical studies of value. The PMBOK shares skills, processes, and procedures for effective project management, offering an industry certification with an unknown rate of industry requirement or published study on its value to the industry or the person obtaining the certification.

*The Standard for Project Management and A Guide to the Project Management Body of Knowledge :* (PMBOK® guide). (Seventh edition.). (2021). Project Management Institute, Inc.

1. Causes and Failure of Projects

A survey of 70 professional engineers (conducted in December 1994 by the author and sponsored by the Faculty Research Support Fund at the University of Houston Clear Lake) suggests that there are at least a dozen distinct explanations for project failure. In this survey, the engineer respondents were presented with 70 postulated reasons for project failure. One major recommendation of this study is that the various stakeholders of the project be included in a very thorough planning process, thereby maximizing the input from the various vested interests and broadening the understanding of the project manager and team members. If realistic goals and objectives are set in the beginning, increased costs, missed schedules, the assignment of inappropriate or substandard resources, and changes can be minimized or overcome, resulting in success rather than failure. In the findings or summary of results, the author never mentioned if they asked the project managers or engineers if they were responsible for setting the criteria for project success or failure within their team, with their stakeholders, or with their clients, but suggests planning is the critical part of the project.

Black, K. (1996). Causes of project failure: a survey of professional engineers. PM Network, 10(11), 21–24.

1. DevOps – Combining Development and Operations

Industry software development efforts have used Agile and development and operations (DevOps) methodologies over the last 5 to 15 years. The Department of Defense (DoD) has applied these. The National Defense Authorization Act for Fiscal Year 2018 (NDAA, 2017) directs acquisition Program Management Offices (PMO) to pursue Agile or iterative software development by establishing pilot programs to use "Agile or Iterative Development methods to tailor major software-intensive warfighting systems and defense business systems.” Memoranda has been published ordering the Air Force to use Agile methods. Agile Development includes the concepts of Continuous Development/Continuous Improvement (CD/CI), a work concept of incorporating regular process improvements in development departments. The creator or inventor of DevOps is unknown, but it is believed to be a Department of Defense initiative, with another branch, called SecDevOps, which is a concept of incorporating security. These are work management concepts and not automated requirements definition and test systems. The concept of obtaining technology is either to develop or to acquire, or to develop for acquisition. The Department of Defense has long since in the business of development, and acquisition, obtaining solutions from industry. The DevOps and SecDevOps incorporate not only agile methods, but also parts of the process groups defined in the PMBOK.

Kramer, J. D., & Wagner, T. J., U.S.A.F. (2019). Developmental Test and Requirements: Best Practices of Successful Information Systems using Agile Methods. Defense AR Journal, 26(2), 128-150. https://doi.org/10.22594/dau.19-819.26.02

1. Strategic Management, Capability Maturity Model, and Project Management

What sounds to be like the integration of strategic management, the capability maturity model (CMM) for software development, and the project management body of knowledge (PMBOK) is a finely authored book that says “Project managers in the future will be given the freedom to select what approach will work best for them on their projects. Rigid methodologies will be replaced by forms, guidelines, templates, and checklists. The project manager will walk through a cafeteria and select from the shelves those elements/activities that best fit a given project. At the end of the cafeteria line, the project manager, accompanied by the project team, will combine all the elements/activities into a project playbook specifically designed for a given client.” Just one paragraph regarding strategic management indicating its level of maturity, suggests lunch in a cafeteria, attempting to combine creative writing with technical strategic educational materials on how to integrate the three disciplines or just a simple prompt of the visual cortex of what is considered a maturity level of some engineers – cafeteria-based selections of intermingled scientific underpinnings called ‘elements.’ It includes concepts of continuous improvement but does not incorporate CD/CI as a fundamental concept or official process to be integrated.

Kerzner, Harold. Using the Project Management Maturity Model: Strategic Planning for Project Management, John Wiley & Sons, Incorporated, 2019. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/capella/detail.action?docID=5703982.

1. ITIL/Software as a Service/Service Oriented Architecture; Technology Terminology and the official process and accepted industry concepts as it relates to IT PM

Service management in the IT area just started to appear in the 1980s when the IT systems and the IT environment increased in complexity. IT services can be defined as a group of “tasks” provided by an IT system or an IT department, that is, IT service can be characterized as the application of specialized capacities on IT assets. As IT’s capabilities grow, in what we create, automate, develop, deploy, and what is planned vs. created the need to define and manage complexity, as well as control its growth.

An IT Service Management Literature Review: Challenges, Benefits, Opportunities and Implementation Practices. (2021). *Information, 12*(3), 111. https://doi.org/10.3390/info12030111

1. Causal Correlation Studies of PMBOK and SDLC, is there an effective model to measure

This study suggests it can measure training manufacturing by comparing management methodologies such as Six-signma, PMBOK, and SDLC, and use scientific measurements to show correlations in location moves in a non-specific project, but does not share project details. A long-term goal in the defense industry is to introduce leading technologies while continuing to integrate software innovations for their respective customers (Danylenko, et al., 2021). According to Danylenko, success within the government, private, and aerospace/aviation software training systems was contingent on measuring the ability to provide dependable, repeatable, and reproducible situations during a controlled simulation environment. It seeks to change or integrate TQM concepts with a new quality control system for a Department of defense simulator. Its results appeared to be scientific ramblings and combinations of approaches, with no actual variables to test in a simulator, other than a creative use of industry keywords for work management and control terms.

“A benefactor from this quantitative ex post facto (causal-comparative) research was illustrating how six-sigma continual improvement tools, PMBoK concepts, and SDM-SDLC methodologies best practices (BxP) had a positive effect on demand by consumers of commercial, the government, and private industry sectors.” The writer suggests it has power to suggest investment in multiple management methodologies using causal correlation, without correlative statistics. The importance and lesson is that if management principles and processes using quantitative and qualitative measurements, should have specific data available that can turned into scientific variables for evaluating the correlation of multi-methods, not the integration of all methods for a simple statement that all methods are worth investment, but specific tests of each method for most cost-effective, based on specific test methodologies, and later measure the project management methodologies, which is a different type of qualitative method, for a different purpose. Knowing the difference is a knowledge indicator of professional skill and scientific test design, rather than fancy persuasive writing.

Mosley, M. D. (2022). Continual Improvements in Information and Technology: A Quantitative Ex Post Facto (Causal Comparative) Study Design (Order No. 30245738). Available from ProQuest Dissertations & Theses Global. (2770014136). http://library.capella.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fcontinual-improvements-information-technology%2Fdocview%2F2770014136%2Fse-2%3Faccountid%3D27965

1. Cost Complexity is Costing You

Finding the root sources of costs is difficult, as they tend not to be directly or exclusively linked to an individual product or even to a particular product family. With the right approach, however, it’s possible to get a solid grip on the true cost of complexity as part of any product development effort. Simplifying complexity is also costing, as is purposely convoluting, deluding, or creating complexity, without an established rule or penalty. Perhaps such efforts have filtered into ‘artificial intelligence,” financial fraud, and poor performance evaluation and reporting methods. Just as finding success, failure, and performance “indicators” or “search parameters” and results using fluid, changing, and multiple methods, with varied scales of human taste, choice, values, and perceptions.

Calculating complexity: Maximizing the value of customization, Chaudhury, et. al, (2021), McKinsey and Company, accessed via the Internet at https://www.mckinsey.com/capabilities/operations/our-insights/calculating-complexity-maximizing-the-value-of-customization.