Sheri L. Wilson

Capella University

BMGT8432 – Project Management Complexity

December 13, 2023

Assignment 10: Project Methodology

Leveraged Identity Authentication

1. Research Topic: Security Interoperability: Simplifying Complexities Using Policy and Project Management
2. Research Problem:

The Internet does not have a shared data architecture that allows for centralized management of personal information. Each Internet Site that is protected by encryption utilizing a profile and account management system is individualized and users create accounts manually, without an automatic profile copy option. Leveraging account management code or functionality from other major applications, tested and proven, such as Facebook and Google, or Id.me has somewhat streamlined the login process, centralized account management and credential use insights are limited and still presented in highly technical terms for users. These complexities and inconveniences present unnecessary security complications which most likely increase the risk of breach. Not only is it a highly duplicative manual process, but each site varies in its information requirements, yet promises the same level of security. The problems are in the architecture, lack of shared and centralized design, and individualized security protocols within each application without a security account management suite. Password management vaults and ‘remember me’ login features are available, but they do not solve the architecture problem; they are quick answers to complex and critical systems that require a shared data solution. Password managers are effective tools that provide convenience along with security, but they are not a cure-all against hackers (Security,org, 2021). Multiple user profiles exist, and the number grows each time a new application with security features is introduced or a new account is established, reaching an unmanageable number which leads to inconsistency, dysfunction, and conflicting information. There is no automatic fast way to update all accounts, or to perform emergency shutdowns, or to cross check information for validity. Each user is left to their own practices of managing information, and for some odd reason, the security industry thinks the everyday human is capable of understanding complex security management. Risk is transferred to the businesses and users, without a set of good common standards and practices. The major problem is that security breaches are made public, as are suggestions for protection of data, yet each individual has the freedom to manage however they want to. Instructions are often present, but lengthy and complex.

3. Background:

The security design is non-standardized with many recommended standards published by the National Institute of Standards and Technology. Some of the concepts, such as encryption, multi-factor authentication, and other security methods are complex, with no technical guidance for developers to refer to when deciding on how to best implement security for their applications. Authentication is one of the major security functions of online systems. It is believed that when an organization uses DevOps or DevSecOps, it utilizes a standard test model incorporating security throughout its process, but it is only presented in broad terms. Many laws govern the protection of personal data, as outlined in the Privacy Act, the Freedom of Information Act, and other Electronic Systems laws. The law is broadly written and does not govern or regulate security practices, other than to say information must be protected. Security is standardized across the Internet, with account creation and the use of Secure Socket Layers (SSL) Encryption for Internet Sites. Each is built individually, most likely with a common code for account creation and the protection of information while stored and in use. Security has advanced to offer multiple options for securing Internet data, but a problem has risen showing massive redundancy that is believed to increase risk.

Researchers from Stanford University and a top cybersecurity organization found that approximately 88 percent of all data breaches are caused by an employee mistake (Tessian, 2023). Interoperability enables the seamless sharing of information and the integration of security systems from different vendors. It is the key to achieving this integration, as interoperability allows organizations to create a holistic cybersecurity approach that adapts to their unique security architecture (CISOMag, 2023). Professionals continue to promote cyber-security awareness and training programs, and no one has brought up that it might be too much to expect an everyday user to manage a high number of accounts with different security requirements. The expectation that people are capable of managing their own, if given instructions only works to a certain extent and it might be proven that human error is the main cause of breaches and is higher than the number of hacked accounts.

4. Research Questions

Is the current system of individualized profile and personal account management the most efficient and secure solution available and has it reached a point of unmanageability leading to higher risk of breach or unprotected and mismanaged personal data? Will a shared leveraged account management system prove to be more effective in centralized information management? Why is this a matter of choice and not a matter of regulation if it affects the national economy?

5. 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. Technical challenges exist in separating the technology test cases of data to the analytical review and legal application. The use case is designed to prove data and privacy management efficiency 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. “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).

6. Project Management

Project Management processes and knowledge areas can be used in Security, for implementation and to provide a framework for the study of security products. Since Security is often a separate function performed by security experts, in addition to software development or coding, the tasks are managed under one project, perhaps with multiple project managers and dependencies. Security tasks can be managed using the project management system of initiating, scoping, scheduling, budgeting, monitoring, controlling, and executing. When studying security products, such as LIA or IUA, a project management approach can be taken. Current methods project management methods for executing or monitoring and controlling processes for a selected knowledge area (scope, time, cost, quality, human resources, communications, risk, stakeholder management, integration, or procurement) are possible when conducting a study on security products but is more suited for the implementation of security products, wherein the scope varies depending upon selection. The LIA security method in comparison to the IUA method can be effectively managed as part of a project but with a much smaller scope, timeframe, budget, and risk. This fact alone is a reason to recommend LIA over the IAU approach for improved management. Evaluating ethical, diverse demographic, and cultural perspectives appropriate for leading projects and programs to a successful outcome within the framework of the five process groups of initiation, planning, executing, monitoring, and controlling, and closing would require the study to include demographics of surveyed participants and or consideration of studying the use of a specific security product's project management activities of the 5 process groups for comparison. This means the study would need to be done with data from a large population to compare cultural differences in the outcomes of one security product.

Security testing and risk management are important tasks that are managed using PM principles. A risk assessment explores how a component could be exploited by the identified threats (i.e., what could go wrong) and analyzes the possible responses to such attacks. The response options for a risk are to (a) mitigate (reduce probability of event, reduce impact, improve recovery), (b) transfer (insurance, contracted agreements), (c) ignore (for low impact and highly unlikely threats), or (d) avoid, which may require changes in requirements (Ellison, 2006). The differences in scope, security, and risk between LIA and IUA are tremendous, affecting all process groups and the project plan. Although still important to test, with a much shorter implementation timeframe, and limited responsibility for code creation and testing, the LIA method greatly reduces risk and the project scope. Seeing the power of automation, managing API has also been handed over to API management platforms or software. Using such platforms, businesses can trim down the efforts, time, and money invested in maintaining the product as well as its API (Wallarm, 2023).

A specific project management methodology such as Traditional, Agile, or other method might be used to manage the implementation of API products. It doesn't matter which method is used, but it must be understood that LIA-API product implementation varies significantly from IUA development and implementation. It can be hypothesized and proven that one method works best for a specific security product, but the research study must stay in scope and only evaluate the use statistics and not development comparisons of LIA and IUA. The significance of API management for developers ensures robust security through authentication, authorization, and encryption measures (Hafeez, 2023), among other benefits. The implementation of an API is part of a software development project, managed using some project management method, but becomes are regular operational security management task that is ongoing. Management of security data takes place on the developer's side and the user's side. This study is mainly focused on user management of security data when using API products; specifically LIAs.

7. Strengths and Weaknesses of Project Management Research

Earlier research conducted regarding Project Management studies is of limited value but do provide some guidance on how to effectively organize the research study. Although no specific research studies regarding project management can be used to support the research questions or prove the hypothesis, they are useful in selecting a specific PM method to use for the research study. There are no specific Project Management studies that are correlated to security products or specific to DevSecOps that could be applied to the two security products selected for evaluation. According to Nidecki, "no matter what name you choose for your secure DevOps, the important thing is to realize that security should not be an isolated island in your development and deployment processes but an integral part of every activity in the software development lifecycle" (Acunetix, 2023).

8. Limitations of the Study

Testing to prove the hypothesis can only be done on a user level or a developer with a user account to test Leveraged Identity Authentication. The test can compare LIA and IUA methods and determine efficiency levels, as well as measurements for information management, but it cannot predict frequencies of forgotten passwords, breaches, or changes in risk using the existing framework because it is a new and different design. Since not all e-commerce or internet sites with a profile and account management system uses LIA, and the Internet is so vast, its only possible to create a test for one user. Once one users experience can be tested and evaluated, the test can be scaled across the internet to see how vast the problem is and how impossible it is to manage Internet Security from a global security perspective.

Choosing the right project management method for implementing a security product is essential. While the complexity of security is greatly reduced using LIA products, implementation and testing are still required, meaning it must be managed as part of the project. The DevOps and DevSecOps incorporates not only agile methods but also parts of the process groups defined in the PMBOK (Kramer & Wagner, 2019).

9. 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 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. 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 as a 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 understood 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.

10. Risk Management

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. Everyday users are not educated in the Risk Management Framework and efforts to train or educate small businesses on such practices is a nation-wide endeavor. The transfer of risk occurs, without effectively explaining the problem and protection measures to users and the metrics for 'security' and information management is not consolidated and reported, so there is no way to truly understand America's Internet Security standings, risks, and problems.

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.

11. Significance of the Study

The study is important to prove that while the Internet enables people to connect across the world and do business, socialize, and complete information tasks, it is not a shared architecture. Because it is not a shared architecture, information is duplicated, varied, and difficult to manage. Users do not have a technical solution for tracking their own activity, data storage, personal information and have a duplicative system for tracking accounts. This study not only shows problems in the architecture, but also shows much efforts towards training and education versus the creation of a centralized automated system for users. Users are expected to be responsible for the sharing of the data, and commerce responsible for the protection of data, yet the management process has become so duplicative and daunting, its obvious that the more data there is to manage in multiple places, the greater the odds are of breach or false information that goes unmanaged.

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.

12. Research Method: Quantitative Research using data collection and statistical analysis to compare the average number of online accounts per user, number of leveraged accounts, and management time. It must also review a small sample of password reset frequency, along with a comparison of two security products. It will evaluate two variables comparatively and statistically: leveraged security and individual security profile management. More variables may be added.

13. Research Questions

Does the individual user account security system suffice for a single user and how does it compare to LIA methods in terms of security, time, management, use, and risk? 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? It is believed and can be proven that the more security options a user's has and the more variation in process, the greater the chance of mismanagement. Forgetting information is not the only problem, but also the inability to centrally manage and effectively share or entrust data to others for management.

14. Data Collection

Data will be collected and analyzed to show differences between leveraged individual accounts (LIA) and individual user accounts (UIA); compared numerically, along with time statistics to measure efficiency. Process must be compared, as well as adherence to the Risk Management Framework, if risk assessed. Confidentiality is important and ensuring safe handling of information and protection of personal data. Specific informed consent will be explained in detail as to the extent of the survey and voluntary participation. Anonymity will be an option for survey participants and published results will not include personal information.

15. 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.

16. Quantitative Research

The number of personal online accounts, as well as a recording of time to access and change data, compared using two solutions: the LIA and IUA. Data management procedures must also be evaluated and compared. The comparisons are not just for the number of accounts and the time it takes to access and manage it, but also a scenario for a data change in comparison of both, along with important questions, such as how to best manage everything in one place, whether there is a technical solution or a paper process, or reliance on memory.

17. 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.

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

2. 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

3. 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

Leveraged Identity Authentication

Informative Article

4. 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

Qualitative Case Study

5. 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.

Qualitative Study

6. 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.

Qualitative Study

7. 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

8. 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%2Ftradejournals%2Fchapter-1-cognitive-information-processing-theory%2Fdocview%2F2573517889%2Fse-2%3Faccountid%3D27965

Scholarly Journal

9. 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

10. 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

11. 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

12. 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.

Leveraged Identity Authentication

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

13. 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

Qualitative Informative Study

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

Leveraged Identity Authentication

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.

Quantitative Research

15. 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.

Quantitative Analysis of Survey Research

16. 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, et. al,. Diversify to Survive: Making Passwords Stronger with Adaptive Policies. SOUPS 2017, Santa Clara, CA, July 12-14, 2017.

Quantitative Analysis of Survey Research

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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

25. 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

Leveraged Identity Authentication

26. 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

27. 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

29. 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."

Leveraged Identity Authentication

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

30. 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

31. Software errors can be introduced by disconnects and miscommunications during the planning, development, testing, and maintenance of the components. The likelihood of disconnects and miscommunications increases as more system components have to satisfy security requirements.

Leveraged Identity Authentication

Software Engineering Institute, Carnegie Melon University, Mellon, R., Security and Project Management, February 2006, accessed via the Internet at https://insights.sei.cmu.edu/documents/431/2013_019_001_297293.pdf on December 12, 2023

Scholarly Article

32. The Concept of API Management

API management tends to alter or modify as per the organizational needs. However, API security, monitoring, and version control are its 3 attributes that your team cannot overlook while creating a strategy for using and improving the API successfully in the long term.

The Concept of API Management, Wallarm Learning Center, undated, accessed via the Internet at https://www.wallarm.com/what/the-concept-of-an-api-management on December 12, 2023

Scholarly Article

33. 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

34. 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

35. 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

36. 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.

37. 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.

38. 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

39. 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.

40. 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

41. 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 are 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

42. 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.