Issues in Information Systems
Volume 22, Issue 3, pp. 62-72, 2021

DOI: https://doi.org/10.48009/3_iis_2021_69-80

A case study in selection and deployment of a multi-factor authentication solution

Elizabeth C. Donald, *University of North Alabama, edonald@una.edu*
Michael A. Bumpus, *University of North Alabama, mbumpus@una.edu*
Xihui Zhang, *University of North Alabama, xzhang6@una.edu*

Abstract

Adapting to an increasing cybersecurity threat is an ongoing challenge for all organizations, with the 2020 global pandemic of COVID-19 introducing additional variables into the security equation. COVID-19 forced many companies to adjust rapidly from on-premises employees to a primarily remote workforce where in addition to physical health concerns, these companies were now faced with network and system health concerns at an unanticipated scale. Simple username and password combinations continue to be vulnerable to brute force attacks, social engineering, and user negligence. Overcoming these security challenges often results in changes in organizational behavior and process as well as the implementation of additional enhanced authentication protocols. One protocol that can offer an additional level of security is known as multi-factor authentication, which relies on a combination of authentication methods to enforce system access policies. This case study will review and assess the selection and deployment of a multi-factor authentication solution within a government contracting organization, outline the challenges encountered during the process, and make recommendations for avoiding pitfalls in multi-factor authentication implementation. Finally, this study will also address the role multi-factor authentication played in company readiness to support a shift to a remote workforce in response to stay-at-home and safer-at-home orders.

Keywords: multi-factor authentication, MFA, two-factor authentication, remote workforce, cybersecurity, COVID-19

Introduction

Prior to 2020 and the rise of COVID-19, working from home was a luxury that relatively few workers were able to enjoy. Many smaller companies who had not heavily invested in the infrastructure and scale-communications to allow for remote employee access to company systems and resources, found themselves struggling to maintain business continuity in the face of a majority remote workforce, driven by social distancing mandates and stay-at-home orders. With the number of remote workers greater than ever before, data security practices are facing new challenges. Compounding the challenges with securing remote access, business continuity and compliance standards require workers to maintain security protocols, no matter their location. Manufacturing facilities are familiar with keeping people safe and must abide by many rules and regulations that are designed ultimately to save lives. These protocols are now compliance requirements and directly impact business operations (Kelly & Popa, 2020).

In this study, we will explore the implementation of a multi-factor authentication (MFA) solution and how it impacts users in both traditional office settings and when working remotely. Through a focus on the challenges and successes within the solution selection and deployment processes this study provides an understanding of the gravity held by such an undertaking and seeks to inform future deployment planning and risk mitigation. Additionally, the sudden COVID-19-driven move from onsite to remote employees is covered to highlight how these MFA practices carry over to non-traditional workspaces where secure authentication becomes increasingly relevant and how security processes evolve to meet these requirements.

Literature review

In the past, data security was centered around physical access to on-premises systems and strong password requirements. What once might have given a business a competitive advantage when trying to win a contract or serve as a siren song for potential investors has become a business-essential necessity. Modern security practices revolve around many types of system authentication and authorization. One such practice is the implementation of a multi-factor authentication solution (Littlewood et al., 1993; Schneier, 2005).

Cybersecurity concerns in the COVID-19 era

Government and business responses to COVID-19 led to the sudden and widespread closure of many physical office locations and forced workers into a remote, work-from-home scenario, seemingly overnight. More than one-third of the workforce moved to remote work during the first months of 2020 (Brynjolfsson et al., 2020). Ongoing shelter-in-place orders extended the remote work for several months, with many still having not returned to the offices full-time. Working from home multiplies cybersecurity concerns as workers and security teams struggle to balance business-continuity needs with access control requirements (Boehm et al., 2020; Brynjolfsson et al., 2020).

The rapid shift to a remote workforce left some workers without company-provided computers, forcing them to utilize their own. These personal devices are often not centrally controlled, monitored, or secured and can increase the risk of introducing cybersecurity vulnerabilities. This response as well as the loosening of access rights can often lead to greater risks of a breach.

Additionally, societal uncertainty during the COVID-19 pandemic has led to a rise in social engineering ploys designed to gain information or access through deceiving legitimate system users as well as attacks on COVID-19 information websites (Boehm, et al., 2020; Weil & Murugesan, 2020).

The long-term impacts of the pandemic-driven office exodus remain to be seen, but many large companies have already committed to making remote work a permanent part of their operations. Some companies, including Google, Microsoft, Facebook, and Salesforce, wanted to make their remote work policies permanent (Manning, 2020). Even among companies eager to return to the office, “only about 1 in 10...expect all employees to return to their pre-pandemic work arrangements” (White, 2021, para. 1).

One method to help curb the threats posed by the remote workforce is the implementation of a multi-factor authentication (MFA) solution. With MFA, an additional layer of security is proved by requesting the user “be authenticated twice before access to requested resources,” reducing the risks of stolen password(s) and “remote impersonation attacks” (Yeboah-Boateng & Kwabena-Adade, 2020, pp. 162-163).

Multi-factor authentication

Multi-factor authentication, also commonly referred to as two-factor authentication (2FA), is where a user must use different methods concurrently to verify that they are who they say they are before being granted access to an information system. MFA solutions could consist of a combination of a one-time-password (OTP), mobile device push to accept or reject the login, or a hardware or software token with a rolling passcode. Authentication factors are broken down into three groups: something you know (a password), something you have (a token), or something you are (biometric data) (Yeboah-Boateng & Kwabena-Adade, 2020).

Two-factor authentication typically consists of something the user has and something the user knows. The user can have a physical token that plugs into their computer or a token generator on their mobile phone, or know a password or a personal identification number (PIN). Combining a token and a PIN to authenticate achieves the two-factor authentication. In the case of a mobile device-based token where the device is unlocked via biometrics, the third layer of authentication is employed by default, provided the mobile device is managed by a trusted organization. MFA ensures a higher degree of security and can grant or deny access based on a variety of possibilities and data points (Karlinsky, 2016; NIST, 2021; Schneier, 2005).

Methodology

Our research focused on an implementation case study of Company A, a Department of Defense subcontractor, their MFA implementation response in the months leading up to and following the widespread COVID-19 outbreak in the United States and subsequent shift to a remote workforce. There were seven implementation phases, and the implementation details for each phase are provided in the next section.

Expectations for this study include revealing the hurdles in MFA implementation, identifying key steps in MFA planning, and factors for successful deployment. Just as mandates for physical security are ultimately set to keep people safe, cybersecurity regulations are ultimately chosen to keep data safe. Cybersecurity is tedious and difficult because attackers are growing in knowledge, strength, and numbers. System users must partner with cybersecurity teams and adopt a security posture to safeguard data before any sort of penetration (McKeown, 2019; Schneier, 2005).

Case study

Company A participates in government contracts and must comply with Defense Federal Acquisition Regulation Supplement (DFARS) Claus 252.204-7012 - *Safeguarding Defense Information and Cyber Incident Reporting*. This clause mandates the use of multi-factor authentication. Company A developed a two-year project plan (beginning in January of 2018) to implement multi-factor authentication for its 2,000 users that utilize the Information System environment. The project stages included analysis of alternatives, proof of concept and interoperability testing, business case proposal, alternative solution evaluation, and testing, funding approval, implementation throughout 2019, and evaluation of lessons learned. This study will describe the implementation process and analyze the lessons learned. For a visual representation of the implementation timeline, see Figure 1.

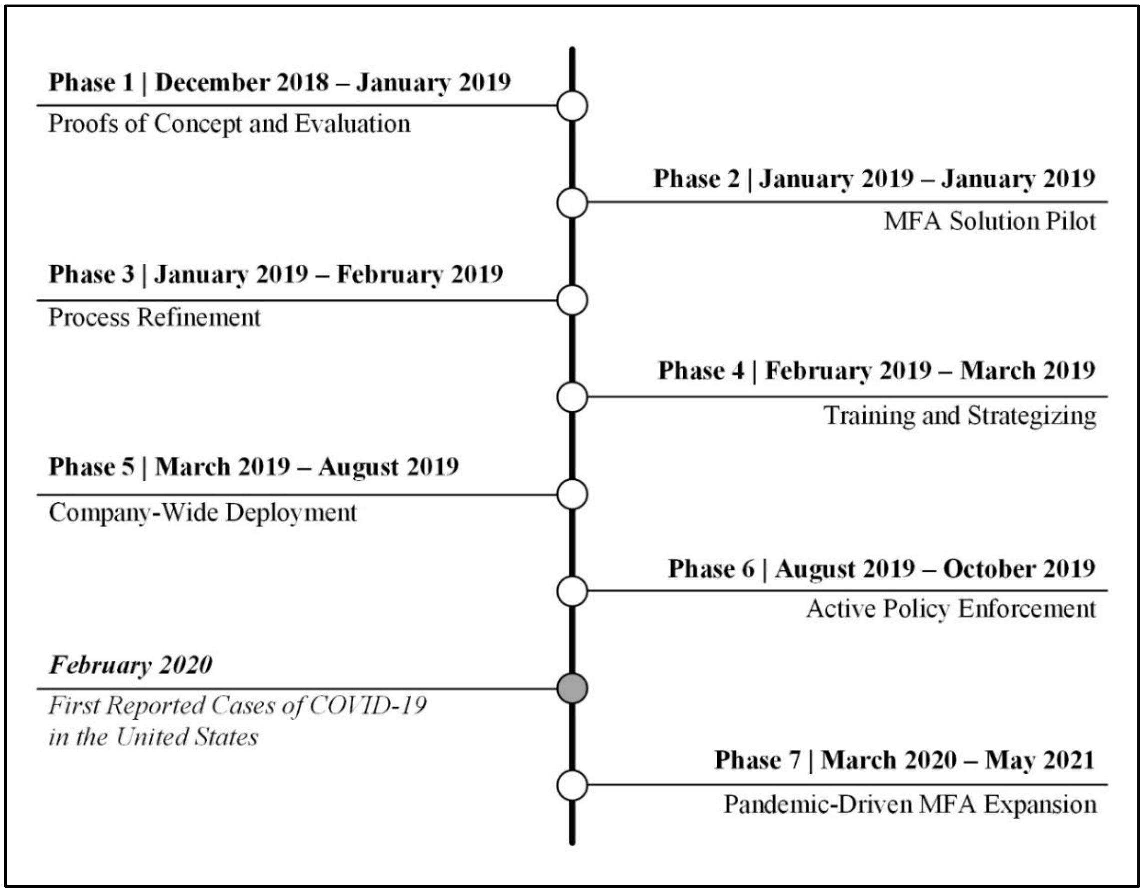
Phase 1 | December 2018 – January 2019
Proofs of Concept and Evaluation
Phase 2 | January 2019 – January 2019
MFA Solution Pilot
Phase 3 | January 2019 – February 2019
Process Refinement
Phase 4 | February 2019 – March 2019
Training and Strategizing
Phase 5 | March 2019 – August 2019
Company-Wide Deployment
Phase 6 | August 2019 – October 2019
Active Policy Enforcement
February 2020
First Reported Cases of COVID-19 in the United States
Phase 7 | March 2020 – May 2021
Pandemic-Driven MFA Expansion

Figure 1: A Timeline for MFA Implementation

Phase 1 – proofs of concept and evaluation

Company A evaluated several platforms for multi-factor authentication. They ultimately decided upon a physical USB token and PIN (token+PIN) combination. Among many elements, the ultimate deciding factor of choosing a physical token over a smartphone application was the lack of a Bring Your Own Device (BYOD) policy. Developing a BYOD policy would have required additional investments in time and finances. Company A leadership chose not to allocate these additional resources for this project. The project required cooperation and participation from several facets of the IT team. IT Security led the efforts, but the server, network, and helpdesk teams were unforgeable assets to the success of this project.

Phase 2 – MFA solution pilot

Company A chose a phased implementation approach. After outlining the process steps, the project team began transitioning IT Security employees from traditional password to the selected token authentication method. The next step was to select the pilot group, coined a Noah's Ark group, consisting of two users from each department. Users selected for the Noah's Ark group were selected based on their responsiveness, comfortability with testing, and acclimation to multiple business applications. Some failed interoperabilities were identified with user applications during Phase 2 and remediation steps taken. Several vendor consultation sessions resulted in impacted applications being updated or reconfigured to comply with the new authentication method. One application used for interoffice instant messaging could not reach a resolution and was removed from the environment entirely and replaced with a compatible solution. After each interoperability issue had been resolved, the project team moved to Phase 3.

Phase 3 – process refinement

Phase 3 was designed to automate some of the required implementation processes to create a more streamlined experience for the users. Early in this phase, it was discovered that while the MFA token driver automatically downloaded upon initial use, the driver would fail following certain Microsoft Windows updates. Users would be prompted to insert the USB token, but the certificates could not be read, and the PIN prompts would not display. Company A's troubleshooting team worked with the vendor's technical support team to develop and apply a new driver. Each token required a time-consuming install of drivers to allow the token to properly communicate with the PC. Prior to the end of the phase, the team had successfully assembled and packaged the required drivers for network deployment via Microsoft System Center Configuration Manager (SCCM), simplifying the installation process.

Phase 4 – training and strategizing

Phase 4 was to create implementation documentation and train the helpdesk team on the newly defined processes. The team also decided to keep the password-only authentication live in tandem with the token authentication until all users were given an opportunity to become comfortable with the token process.

The helpdesk documentation included steps of checking the driver settings and applying them if they were missing. If the user had been offline during the SCCM driver update pushes, they would need the driver manually installed when they received their token.

The available user documentation generated for the phase was limited, requiring a more hands-on engagement from the helpdesk team. Users were shown where to plug their tokens in and how to create a unique PIN. Helpdesk team members remained available to assist with troubleshooting token issues and the deployment teams moved into Phase 5.

Phase 5 – company-wide deployment

During phase 5, the teams began to deploy the MFA solution to all employees. An iterative model was implemented for the rollout, following some tenets of Agile methodology through end user involvement, incremental delivery, and embracing change (Mairon, 2019). The groups selected for each iteration were based upon job type and user location. Utilizing Agile for solution deployment was not standard practice for Company A's IT team but was selected to allow them to evolve processes and training procedures as the deployment progressed. Company A's leadership determined the process should start by introducing MFA to users that were close in physical proximity to the IT Department in case there were any catastrophic or lingering issues; the implementers could reach those having trouble quickly and resolve their authentication issues. The end users of this first iteration group were also considered more "tech savvy" and leadership believed would be able to better understand any issues and articulate them effectively. This gave the deployment team the opportunity to review their work and adapt the rollout plan to become better with each increment. A breakdown of the end user groups selected for each increment is found in Table 1.

Table 1: MFA Agile Deployment Increments

Deployment Increment	Department Involved
1	● Remaining IT Users ● Accounting ● Supply Chain
2	● Main Office and Administration Building Engineers ● Human Resources ● Legal
3	Manufacturing Building Engineers
4	First Half of Manufacturing
5	Second Half of Manufacturing
6	Remote Site Workers

The first group consisted of the remaining IT users in the main office complex, the Accounting department, and Supply Chain personnel. The second group included the engineers in the main office complex and administration building. The HR and legal employees also received their tokens in group 2. Group 3 added the remaining engineers assigned to the manufacturing buildings. Groups 4 and 5 each took half of the manufacturing users. The remaining user groups encompassed the users at the three remote sites. These remote sites each have dedicated site-to-site Virtual Private Network (VPN) maintaining an always-on connection to the corporate networks, as opposed to a client VPN that would only connect when the user was utilizing the tunnel application.

Tokens were distributed en masse to each group. For users in the office complex, helpdesk and IT Security personnel set up stations to distribute and demonstrate token use. The administration building received a similar approach, the use of a common office space and a mass distribution.

Group 3 was more challenging due to the quantity of users and their work location proximity to IT resources. The manufacturing areas abide by a strict schedule and the employees are given scheduled breaks throughout the workday. All manufacturing employees take these breaks at one time to keep production running at full capacity as much as possible. The deployment team utilized this break schedule to set up stations in the large break rooms on the manufacturing floors. Tokens were again distributed en masse with a few moments of training. This approach gave employees an opportunity to openly ask questions outside of the normal, ticket-based-helpdesk process.

Phase 6 – active policy enforcement

Phase 6 was to enforce MFA adherence for all users. This meant that users would no longer have the option to use only a password to log in. Their token+PIN combo would have to be utilized to gain access to any of Company A's information systems. Users were advised to call the helpdesk or submit a ticket if they had any issues getting logged in. The six-phase approach to MFA implementation had some challenges but was deemed an overall success by the IT team and company leadership. Company A successfully moved every user to a token+PIN authentication method, applications were configured for compatibility, and users were trained.

Phase 7 – pandemic-driven MFA expansion

Company A had to unexpectedly add a phase 7 to the MFA implementation project. Shortly after completion of phase 6, the COVID-19 pandemic hit the United States requiring strict social distancing guidelines for all organizations (Bialek et al., 2020). Many mandates were set, and people were encouraged to stay home. Company A was deemed an essential workforce and was not required to send all employees home. They did, however, take every precaution seriously and took steps to offer remote work for their upwards of 2,000 information system users.

Prior to the MFA deployment, Company A had a client VPN configured and functioning, but it was only utilized by IT personnel and a few traveling employees. To facilitate working from home, the MFA solution was configured to authenticate against the VPN service, providing secure, remote access to company network resources. According to Chávez (2020), this combination of "encryption and security technologies for the [remote] connection reduces the risk of cyber attacks" (p. 2). Prior to deployment, this augmented VPN solution also had to go through proper testing and change management procedures to comply with company policy. Once testing was complete, users had to be trained en masse during the pandemic. The training was done through thorough instructional newsletters and a heavily engaged helpdesk team.

The server team also configured an additional, more cost-effective virtual remote desktop platform that integrated with the chosen MFA method. The security team assisted in processing helpdesk tickets to more quickly enable the majority of the workforce to successfully work from home. Under normal processes, this type of deployment would typically take several months, however Company A was able to get all new work-from-home (WFH) users online and mostly comfortable. This abrupt change took Company A's workforce from 0% WFH to 70% WFH in three weeks. Company A attributes this successful migration to a dedicated, well-trained, intuitive Information Technology team.

Challenges and recommendations for MFA implementation

Company A found three areas, including culture, processes, and resources, where lessons were learned throughout the implementation process. Both successes and failures were identified in each area. This case study also brings to light several specific findings around key success factors for MFA deployment and implementation. These have been reviewed and redesigned as recommendations for each designated area. These recommendations should guide new MFA deployments to a successful implementation.

Overcoming cultural challenges

Developing a change-culture

IT personnel experienced some resistance to change during the process from both end-users and IT staff. "The afforded data and information assets in digital systems are more visible, accessible, and vulnerable for motivated offenders" (Li et al., 2021, p. 226). Relaying this thought to non-IT personnel was simple, but inspiring others to adopt and believe in the change was more challenging. Once the project began, changes were needed that had not been identified before implementation. This caused some unintentional and unexpected pain points. Success was met when IT staff addressed the need for the abrupt changes, provided possible solutions and lending hands, and easily adapted to the changes. Process interruptions occurred when changes were met with resistance. For example, the App development team at Company A requested an exemption from MFA enforcement. Prior testing and troubleshooting could have prevented discomfort and solutions could have been provided. Instead, frustrations were relieved with a temporary exemption from MFA for the resistant teams.

To improve the organization's perception of change, a culture of change should be adopted throughout the organization at all levels. This allows for a more open attitude toward change as a resource as opposed to a challenge. These outcomes can be achieved by mentoring IT staff on problem-solving, optimism, organizational agility, and innovation. Training videos and team lessons targeting these topics should be instituted. Vey et al. (2017) acknowledged the need for targeted training: "professionals should critically assess the content and learning tools (methodology) of any existing change management training and offerings to determine whether they are topical and correctly reflect the organization" (p. 27).

Providing thorough user training

According to Villanueva and Brewer (2020, p. 2), "employee training [is] crucial in ensuring that security policies and procedures are being properly applied," and this became evident during Phase 5. As company-wide deployment progressed, training became an important topic. Unfortunately, there was no formal funding allocated for training. The token vendor provided some training, but it was deemed insufficient for Company A's users and culture. Even with limited funding, Company A found successful user training results from directional handouts, a dedicated in-house helpdesk, and roaming spot-assistance technicians. These technicians moved throughout the office spaces to provide hands-on training and assistance in real-time. The helpdesk observed a 10% increase in user tickets, all of which were related to MFA implementation. Challenges observed with the employee user training could be offset with additional training resource assignments. It is recommended that user and technician training be included in both the financial and time budgets.

Missed opportunities during pilot phase

An unexpected challenge was noticed when training the workforce to use the new authentication methods. The implementation team utilized a Pilot group to run through the process before deploying to everyone. This successful dry run gave technicians a false sense of optimism in the handouts that were developed for hands-on training during implementation. Those selected for the pilot group primarily consisted of IT personnel that would be considered more tech-savvy than the average user and this group found the handout easy to follow. However, during Phase 5, it was discovered that the handout was insufficient for many less-technical users, requiring a shift to accommodate additional hands-on training.

Pilot groups should consist of users from each department to ensure a true sampling of the population and consequently appropriate development and adaptation of procedures. "An important lesson learnt was the need to include in the pilot and initial phases a cross section of users that used different devices and operating systems or who worked remotely" (Tetlay et al., 2020, p. 11).

Developing effective processes

Planning and defining requirements

During the project planning process, requirements were identified on how to satisfy functional compatibility and user experience requirements with the proper financial budget, time budget, and performance standards. However, criteria were not weighted to reflect the greater impact or importance of each requirement. Most requirements were satisfied, but the cost was a driving force that caused some functional requirements to be disregarded. It is recommended to develop a weighted scale for requirements to best articulate needs and resources that should be allocated to satisfy those needs.

Following the communication plan

IT Security held meetings for the IT Staff, which were utilized to give status reports and troubleshoot issues. Bi-monthly meetings with the IT Steering Committee were held to give status reports and receive guidance from controllers. Meetings with the Board of Directs occurred quarterly as well. IT Security also spun up meetings to discuss issues, perform training, answer questions, and troubleshoot issues as needed. This open line of communication served the team well. All members knew how to get their concerns heard and resolved. Some members did report that the frequency of the meetings caused unneeded redundancy and hindered progress.

According to Mepyans-Robinson (2006), “Effective communications can be the deciding factor of a successful project” (p. 172). Deployment teams should formally develop a communication plan that includes dates for the meetings, outlines for communication to end users and reporting frequency and format to relevant stakeholders (Mepyans-Robinson, 2006).

Meeting resource requirements

Budgeting for success

Funding and cost requirements were identified and approved prior to implementation. However, during implementation, the budget was reduced as it seemed that the original allocation was deemed oversized. This stemmed from the team budgeting for an annually recurring license fee that turned out to be a one-time purchase fee with a much lower recurring subscription cost. While this was welcome news, the misallocation of resources likely impacted other projects. Project leadership should better define the difference between CapEx (capital expenditure) and OpEx (operational expenditure) budgeting to teams outside of the finance department. Decision-makers should receive training on how to properly request and interpret quotations.

Assigning ownership of project tasks

IT Security led the efforts for MFA implementation and was held accountable for each task and subtask regardless of its members’ responsibility and knowledge of implementing that task. The project overlapped every IT team and task responsibilities were shared. Accountability was not shared. MFA implementation was the top priority for the IT department as a whole, but individual teams had differing internal priorities. Project managers should define priorities and synchronize them among all IT Teams. A RACI (responsible, accountable, consulted, and informed) matrix should be utilized to assign responsibility and accountability for each work item.

Conclusion

This study has examined the processes utilized and challenges faced during the implementation of a Multi-Factor Authentication solution. Additionally, these challenges have been paired with recommendations to offset their impacts. The case study also revealed how change implementation must be adaptable to meet evolving business needs and how formal project management practices can help anticipate and respond to challenges. Finally, this study identified additional information security issues exacerbated by COVID-19 and how the company adapted newly implemented MFA solutions to meet work-from-home needs. While delivering an MFA solution was the goal of this project, the IT team was also able to develop and learn from new deployment, project, and change management processes. Future research could continue the examination of MFA implementation across a variety of industries for comparison against this team’s findings.

References

Bialek, S., Bowen, V., Chow, N., Curns, A., Gierke, R., Hall, A., Hughes, M., Pilishvili, T., Ritchey, M., Roguski, K., Silk, B., Skoff, T., Sundararaman, P., Ussery, E., Vasser, M., Whitham, H., & Wen, J. (2020). Geographic differences in COVID-19 cases, deaths, and incidence – United States, February 12-April 7, 2020. *Morbidity and Mortality Weekly Report*, *69*(15), 465-471.

Boehm, J., Kaplan, J., & Sportsman, N. (2020, March). Cybersecurity's dual mission during the coronavirus crisis. https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis#

Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H.-Y. (2020, June). COVID-19 and remote work: An early look at US data. https://www.nber.org/system/files/working_papers/w27344/w27344.pdf

Chávez, J. D. (2020, April). Key considerations for ensuring the security of organisational data and information in teleworking from home (Thesis). Departamento de Informática, Universidad Politécnica Territorial del estado Aragua, Venezuela. https://www.researchgate.net/publication/340389338

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems*, *38*(1), 222-245.

Karlinsky, E. (2016, December 9). Two-factor authentication vs. multi-factor authentication: What are the risks? https://www.okta.com/blog/2016/12/two-factor-authentication-vs-multi-factor-authentication-what-are-the-risks/

Kelly, B., & Popa, R. A. (2020, August 7). Higher education research, cybersecurity, and CMMC compliance. https://library.educause.edu/resources/2020/8/higher-education-research-cybersecurity-and-cmmc-compliance

Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., McDermid, J., & Gollmann, D. (1993). Towards operational measures of computer security. *Journal of Computer Security*, *2*(2-3), 211-229.

Mairon, K. (2019, October). *The Agile Model-Driven Method* (PhD Thesis). The University of Plymouth. http://hdl.handle.net/10026.1/15257

Manning, K. (2020, August 28). 20 organizations never returning to the office. https://www.processmaker.com/blog/20-organizations-never-returning-to-the-office/

McKeown, D. (2019, April). Building a risk-based information security culture. *ISSA Journal*, 14-21. https://donmckeown.net/Building_a_Risk-Based_Information_Security_Culture_-_Don_McKeown-4-2019-ISSA_Journal.pdf

Mepyans-Robinson, R. (Ed.). (2006). Chapter 13: Project communications management in practice. In *AMA Handbook of Project Management, Second Edition* (pp. 165-173). AMACOM.

NIST (2021, April 19). Back to basics: Multi-factor authentication (MFA). https://www.nist.gov/

itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

Schneier, B. (2005). Two-factor authentication: Too little, too late. *Communications of the ACM*, *48*(4), 136.

Tetlay, A., Treharne, H., Ascroft, T., & Moschoyiannis, S. (2020, November). Lessons learnt from a 2FA roll out within a higher education organisation. https://arxiv.org/pdf/2011.02901.pdf

Vey, K., Fandel-Meyer, T., Zipp, J. S., & Schneider, C. (2017). Learning & development in times of digital transformation: Facilitating a culture of change and innovation. *International Journal of Advanced Corporate Learning*, *10*(1), 22-32.

Villanueva, L., & Brewer, D. (2020, March 30). Managing remote work environments with COBIT 2019. *COBIT Focus*, 1-4. https://www.isaca.org/resources/news-and-trends/industry-news/2020/managing-remote-work-environments-with-cobit-2019

Weil, T., & Murugesan, S. (2020). IT risk and resilience - Cybersecurity response to COVID-19. *IT Professional*, *22*(3), 4-10.

White, M. C. (2021, January 26). Just 1 in 10 companies expect all employees to return to the office. https://www.nbcnews.com/business/business-news/just-1-10-companies-expect-all-employees-return-office-n1255589

Yeboah-Boateng, E. O., & Kwabena-Adade, G. D. (2020). Remote access communications security: Analysis of user authentication roles in organizations. *Journal of Information Security*, *11*(3), 161-175.