Leadership Challenges When Managing and Securing a Corporate Enterprise During a Pandemic

Dr. El Gbouri, Abdessamad, Washington, DC

Michael Pry, Latrobe, PA

Dr. Scott Mensch, Saltsburg, PA

Abstract

How do we better secure remote endpoints for both computers owned by the corporation and owned by the employees? How do we train and oversee the human factor in cybersecurity and address risks of employees' online behavior when they work from home? How do the above 2 points change the role of the CISO and the need for new levels of organizational authority? How can the CISO be successful in a cross matrix – dual reporting relationship situation? Finally, given the cybersecurity risk to critical infrastructure and that most of the critical infrastructure is owned by the private sector, should NIST also publish guidelines for the design of the CISO role just as they have done with the role of the cyber security analyst via the NIST NICE framework?

Keywords
Distributed workplaces, Business Continuity Planning, BYOD Policies, Remote Access

I. INTRODUCTION

The societal shift caused by the COVID 19 outbreak caused a global impact including critical infrastructures. The suggestions from this study provided a unique new way to consider telework and remote computing as a requirement for future employees and added new considerations for the information security roles within organizations. Although policies are made to manage programs by providing a framework for governance, identifying, and treating risk, and defining compliance [1], future policies should be aimed to not only manage the program but increase its chances of success and growth when changes come.

II. PROBLEM STATEMENT

The problem is that a new security challenge has emerged for today's cybersecurity leaders. In the post covid-19 era the dynamic of work has changed across the nation with many employees now working from home. Unlike the controlled environment that existed when employees worked from the office, the work from home employee presents a challenge with the security of the end point computers they are working on. Organizational leaders must develop new methods to maintain visibility of all devices connected to their network and to have strategies to secure them. Organizational leaders have always been challenged with adapting their organizations to changes in the environment. In the post Covid 19 era, one of the changes to the business environment is migration from office work to working from home. Prior to the Pandemic, only 7% of workers nationwide enjoyed the benefit of telework in contrast to 71% in the post Covid era [2]. With these new workforce characteristics, corporate cybersecurity leaders must acknowledge the change in how workers access network resources and adapt their security strategy to accommodate this change.

III. BYOD CONSTRAINTS, RESPONSIBILITIES, AND LIMITATIONS

To better identify the major themes considered in studying information security, it is crucial to think about how the industry-leading professional entities have divided the areas of concerns for cybersecurity. From this viewpoint, reference [3] outlined several security domains. Understanding these domains provides an idea of the

elements of information security that should be considered when drafting any policy that has the ultimate objective of strengthening the organization's security posture. When considering BYOD technology information security implications, these domains will come into play, from asset management to governance and risk management. All domains should be considered in evaluating the extent of the BYOD solution in affecting an organization's information security.

Since the success of any solution comes primarily from the response of the workforce towards the benefits and ease of use of the solution or its "appeal" to use as presented by the CISOs and similar stakeholders, and as explained under the Unified Theory of Acceptance and Use of Technology (UTAUT) [4]. Veiga and Eloff explained the aspects that relate to information security governance [5], offering a new framework on the governance of information systems management. Veiga and Eloff explained the main objectives for information security programs, including protecting, safeguarding information, and ensuring the CIA triad: confidentiality, integrity, availability. This document provided starting points to probe while conducting the interviews that were planned for this study.

Information security academic research in the present era has presented advantages, disadvantages, and challenges [6]. The advantages that have emerged relate to the abundance of research material and extensive studies in information security [7]. Knowledge databases on the topic are more readily available, including the plethora of cybersecurity vulnerability databases (National Vulnerability Database - NVD, National Institute for Standards and Technology - NIST and similar). Tech Giants periodic Reports such as Gartner, Verizon, and similar. The disadvantages related to research into information security are generally the rate of advancements in information security technologies, making the relevance of studies harder to accept and validate. Often, research is irrelevant by the time a study is published. In other words, by the time the research is completed on a certain topic, the technology advances and that topic becomes obsolete. Researchers may relate old research to support their claims; however, the cited facts of the study could simply be no longer relevant to the actual capabilities of the studied IT solution. In the case of BYOD technology, its capabilities, risks, span, and scope have morphed throughout the years, where some risks have been resolved, others have been added, especially the risks related to end-users' behaviors, including risks related to cloud services [8].

IV. BYOD OVERVIEW AND BENEFITS

BYOD technology has been adopted worldwide because of its benefits to employees and organizations [9]. "BYOD can be described as the usage of personally owned devices for work purposes by employees" [10]. According to [11], the objective of BYOD solutions is to allow access to organization platforms and tools, such as productivity applications, email, and databases to access and manipulate organizational information. Because of the global connectivity made possible by the Internet, organizations involved in smartphone manufacturing and applications development have also designed solutions within the guidelines of government regulations. Generally, governments must negotiate technical specifications locally and then often within cross-border treaties [12]. One of the latest guidelines with global impact has been the European Union's General Data Protection Regulation (GDPR) [13], which are laws and articles drafted by European countries to protect their citizens' privacy.

Cyber-attacks are generally low cost and difficult to trace, giving "state actors the perfect venue to engage in malicious activity without fear of attribution or retribution" (Tran, 2018, p. 381, para. 1). This ease of execution, along with the global aspects of government BYOD solutions, make governments more prone to being targeted by ever-evolving cyber-attacks, particularly "state-sponsored cyber-attacks, since they have the potential of causing significant and wide-ranging harm across a number of critical areas" [14]. A few of the most famous state-sponsored attacks include Stuxnet (attack on a nuclear infrastructure), the Sony hack (attack on a commercial tech giant), the Estonia DDOS attack (attack on a government infrastructure), and the Mirai botnet attack (attack on the Internet infrastructure itself). These new global security aspects and a heavier reliance on mobile technologies make the capabilities of the BYOD technology more important to study in an effort to draft a more effective policy framework.

V. BYOD ADVANTAGES AND DISADVANTAGES TO THE EMPLOYEE

According to reference [15], employees are more comfortable and generally more satisfied when they can use devices and software or mobile applications that they are most accustomed to from anywhere. In addition, employees do not see working from their own devices as "work", which makes managers appreciate BYOD solutions, since they can see the performance of their employees go beyond paid working hours [16]. [17] outlined a plethora of challenges when implementing a BYOD program. Privacy is a disadvantage for the employee, since not only organization data privacy but the employee's data have to be safeguarded [18]. Another area of concern is the awareness of privacy self-protection [19], especially since employees are left to ensure the security of their own devices [20]. In addition, the blurred boundaries between personal and work data constitutes a privacy risk to the employee due to intermixed data accessible by the organization, and a security risk for the organization either through "data loss, loss of control, and violations of industry regulations" page 28 or [17].

VI. BYOD BENEFITS TO THE ORGANIZATION

In an age of fierce competition, organizations focus more on process improvement initiatives that have evolved over the years to Total Quality Management (TQM), Six Sigma, Lean, and finally Lean Six Sigma processes. The ultimate goal of these processes is to "improve a company's operational performance, processes, business practices, and operational support systems" page 1 of [21]. These process improvements or innovations are vital for an organization's survival [22]. Increased innovation is one of the benefits of using the BYOD technology, as inferred in a study completed by Koffer, Anlauf, Ortbach, & Niehaves [23], where 486 European employees from large-sized companies were surveyed. The results showed that allowing the use of privately-owned IT assets exerts a positive effect on the employee's innovation behaviors. [23] inferred the same regarding BYOD strategies, suggesting that diffusion of consumer IT within the enterprise promotes innovation in the organization. As an IT solution, the use of privately-owned devices for work can have many unintended negative consequences for the organization. For example, end-users and managers could engage in IT consumerization, or what is known as shadow IT, without involving the organization in the decision-making process [24].

VII. BYOD CHALLENGES AND RISK MANAGEMENT

Despite the brilliant efforts of software developers to protect information, their work is often matched by the cleverness of codebreakers as explained by Ekert and Renner in [25], the authors added that although RSA, the most utilized public-key cryptographic system, is extremely hard to break, the system will become insecure when technology produces the first quantum computer. The same will be the fate of many other public-key cryptosystems. This concern indicates the continuous risks to organizations, not only to internal information security strength but how risky the use of uncontrolled and unmanaged devices allowed to access the organization's information systems. These worries should lead organizations to establish several mitigation strategies, including security awareness [26].

Additional risks are related to strict adherence to the use of consumer devices. These stringent policies could lead to security holes since users will always find a way to bypass organizational guidelines [27]-[28]. This aspect is particularly important when dealing with life-threatening considerations, as is the case in the military. [27] reported an incident where a U.S. Army Captain "developed a smartphone application for the use in the battlefield faster than every organizational development initiative from US military could have done it" (p. 206, para. 8). Although this solution, reported in [27] to be better than the government could have imagined, would still have to overcome the outdated policies in place, which they would have affected its legitimacy as a consumer solution.

Other risks include the ease to deploy malware on mobile devices enrolled in the BYOD program. Such malware could communicate with military Command and Control sites, avoiding organizational security safeguards. A prominent threat intelligent report showed that Android devices had seen 31% increase in malware attacks between 2017 and 2018 [29]. Deception could be the weapon of choice to exploit some of the features of mobile devices. Android, for example, builds part of its security on the "permission restricted access model". This concern means application developers would have to abide by the rules of disclosing what permissions their application needs when being installed on an Android device. However, unscrupulous developers could take advantage of this feature and request more permissions than what they need. These malicious applications are termed "over-privileged

applications” [30]. The device itself could be a source of concern when it is lost, stolen, or when targeted by a hacker aiming to gain access to controlled information. In addition, policy violations could cause weaknesses that could be exploited by third parties with criminal intent [31]-[32].

VIII. PRIVACY CONCERNS

Reference [33] stated that “very few papers on privacy mechanisms consider the private data over the untrusted network aspect”. The authors discussed the latest ways to preserve privacy, including the many high-end solutions used for Android platforms with the aim to “give visibility to the device users over how their sensitive data is handled” or to allow users to mask or hide their private data, such as their location, contact lists, and photos and personal information through traffic monitoring technologies.

IX. FEASIBILITY AND IMPLEMENTATION

[34] reported on a study where 315 security professionals, working for organizations of 1,000 employees and up, were asked about their difficulties concerning mobile security. The data revealed that users needed the technology to stay productive, yet there was no lack of challenges when implementing the BYOD technologies. The respondents to the study revealed the main problems were:

- 48%: "Enforcing security policies for mobile devices"
- 46%: "Lost or stolen devices containing sensitive data"
- 46%: “Sensitive data confidentiality and integrity protection when accessed or stored on a mobile device"
- 41%: "Threat management on a mobile device"
- 41%: "Supporting new device types"
- 40%: "Creating security policies for mobile devices" (para. 3)

The same study also revealed that security vendors needed to think broadly about solutions that would encompass all challenges, such as mobile device management (MDM), data loss prevention (DLP), anti-malware solutions, education, managed services, and professional service for mobile device security.

X. GOVERNANCE AND POLICIES

Reference [23] suggested a comprehensive approach to drafting a BYOD policy. The policy is divided into three groups: The operational layer, tactical layer, and strategic layer. Some milestones are being shared between layers. For example, the identification and access control policy is in between the operational and the tactical layer. Many other professional entities have tried to create templates for BYOD policies [35].

For governments, mobile devices will be predominately used for work, meaning that Bring Your Own Device programs will be even more important for governments, businesses, and organizations alike, including the military, as indicated in [36] and further explained [37], which addresses the use of personally owned computers on unclassified USDOD systems and networks. Compared to the private sector, the public sector has not been taking full advantages from IT consumerization. A study was reported showing that 45% of employees in the private sector have the autonomy to choose IT on their own versus 32% in the public sector [28].

Reference [36] also introduced in its strategy the meaning of a secure mobile framework or SMF that enables the organization to identify mobile device requirements. The framework also outlines why this strategy is significant for the organization and its information security posture. This strategy is also of important for the present study because it relates matters of primary concern for the BYOD program. These elements will be considered when analyzing the entire system to understand the perceived controls when establishing this research theoretical framework and aligning it with the revealed themes of the study.

XI. EMPLOYEE COMPLIANCE WITH BYOD POLICIES

Many studies have been done with the aim of outlining the possible solutions to align information security protections and the needed BYOD policies. Reference [38] reported that organizations should be able to prioritize and control the resources and information accessed by employees via BYOD solutions when they enact BYOD information security policies. The same outcome was supported by [39]. As previously outlined, the success of the BYOD program relies heavily on the level of satisfaction employees expect from it [40]. This satisfaction is however influenced by how detailed and clear the requirements definitions when relating the information security policies to end-users [41]. However, many policies cause the opposite effects on employees when requirements become more of a stressful obligation that the end-users must comply and cope with [42].

XII. ORGANIZATION BYOD POLICY ENFORCEMENT

Information security mobile application and device policies are only effective if they are enforced to the point that they are not ignored, they are respected, and, finally, complied with [17]-[43]. The goal is to safeguard information against leakage, spillage, or by causing data breaches. [44] talked about the unrealistic optimism on information security management, this study also outlined the phenomena that increase vulnerability to information breaches. Surveying managers in information security, Rhee and the authors in this study found that these vulnerabilities are linked to the lack of managerial commitment and awareness to consider information security threats at every level of information management.

XIII. THE NEED FOR BYOD POLICY FRAMEWORKS

Understanding this framework can give an insight into the elements to focus on when planning for implementing a BYOD policy-specific framework. The NIST cybersecurity framework has three components: 1. Implementation tiers; 2. Framework core; and 3. Profiles. The tiers component (four parts) shows at what stage the organization is when it comes to its rigor to achieve information security (Tier 1 - Partial, Tier 2 - Risk-informed, Tier 3 - Repeatable, and Tier 4 - Adaptive) [45]. The framework core identifies functions, categories, and subcategories to be managed by all levels of the organization. The high-level functions are designed to identify, protect, detect, respond, and recover. The categories and their subcategories are illustrated in Figure 1 also illustrated in [45].

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
What safeguards are available?	Protect	Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Figure 1. Functions and Categories NIST Cybersecurity Framework Core Component

Note. Adapted from National Institute of Standards and Technology, "Functions and Categories and an Example of NIST Cybersecurity Framework Core Component". [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/Cybersecurity-Framework-Overview/images-media/NIST%20CSF%20Overview.pdf

As mentioned above, [31] had suggested a BYOD policy framework with three layers: operational, tactical, and strategic layers. The current study has per aim to draft a more comprehensive BYOD policy framework that considers not only these three layers but also any layers that stem from assessing the users use of technology and the possible resistance or appeal they have for mobile or remote access via privately owned devices. The scientific method used is assessment via a qualitative study conducted through interviews of a population sample of 250 users.

Theoretical Foundation: The prominent theory that was the basis for this present study is the Unified Theory of Acceptance and Use of Technology (UTAUT) [46]. This theory is the most widely used model to study the reasons behind certain behaviors of accepting or denying a certain technology. This model is based on four constructs:

Performance Expectancy: What benefits would the user expect from using this new technology?

Effort Expectancy: How easy would this technology be to use by the consumers and end-users?

Social Influence: The perception of an end-user as to how a certain technology is seen by others as useful and appealing.

Facilitating Conditions: The perceptions of end-users of the available resources or support to use the said technology.

Understanding the UTAUT constructs related to the present study gives a fundamental view of the aspects that could engage or disengage end-users from enrolling in the BYOD program in this proposed solution.

The open-ended question used during the participant interviews sessions were selected as a starting point for conversation, to gauge the participant's understanding of the question, and ultimately excite the participant's thinking and insight.

Understanding the UTAUT constructs related to the present study provided guidance in participant engagement during the interviews.

Study Findings: the ranking of themes revealed in this study following the UTAUT elements is provided below:

Ranking of Themes by UTAUT Elements.

	Revealed Themes	Rate Mentioned
Effort Expectancy (EE)	Convenience	16%
Performance Expectancy (PE)	Data Security	13%
Performance Expectancy (PE)	State Information Security	9%
Performance Expectancy (PE)	Protection of Privacy	9%
Effort Expectancy (EE)	Ease of use	9%
Facilitating Conditions (FC)	Trusting the Organization Culture of Perfection	5%
Facilitating Conditions (FC)	Risks to the Organization	3%
Facilitating Conditions (FC)	Cost of Non-Compliance / Legal Concerns	3%
Facilitating Conditions (FC)	Risks to the Member	3%
Performance Expectancy (PE)	Productivity	2%
Performance Expectancy (PE)	Mobile Applications Permissions	2%
Social Influence (SI)	Reviews	2%
Facilitating Conditions (FC)	Organization Furnished Equipment	2%
Facilitating Conditions (FC)	Two phones in one	2%
Facilitating Conditions (FC)	Advanced Collaboration Tools	2%
Facilitating Conditions (FC)	Awareness Training (all Forms)	2%
Social Influence (SI)	Organization Culture	1%

Note: Results of the Study Conducted by EL Gbouri (2021) using the UTAUT construct to assess the acceptance of the BYOD technology. Other themes were revealed but at very low rates of appearance in the study interviews.

Upon further analysis of the study finding the UTAUT elements were ranked as follows:

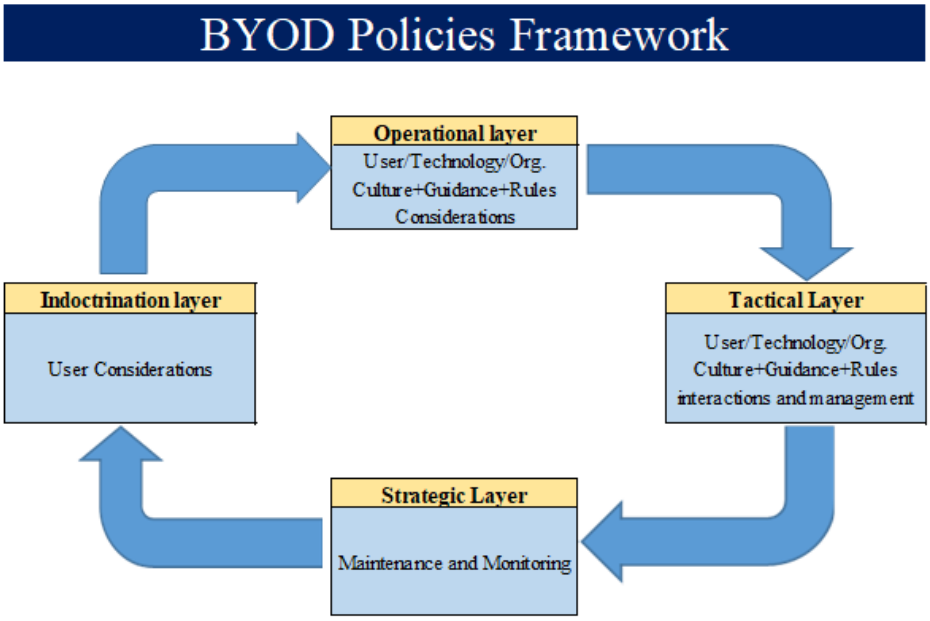
UTAUT Element	% of revealed Themes	Rank
Performance Expectancy	36.66%	1st
Facilitating Conditions	32.66%	2nd
Effort Expectancy	24.66%	3rd
Social Influence	6%	4th

57% of the revealed themes were in the "facilitating conditions" category, and 43% were in the rest of the categories combined. Within the facilitating conditions," the most dominant theme was "trusting the organization culture of perfection".

A Newly proposed BYOD framework: The use of the UTAUT model as the underlying basis for developing this study revealed important insights related to end user acceptance. As an example, if the theme "trusting the organization culture of perfection" is considered by the organization and a mitigation strategy is implemented early enough in the process, the BYOD enrollment rate could be higher. The policy where this theme could be implemented is during the onboarding policy. This consideration drives the necessity to add a new layer before the operational layer where onboarding resides. Other considerations for end user acceptance or disapproval of the program could include a way to validate prerequisites for enrolling into the program or ways to validate the end-user's commitment to data protection, abiding by the business rules, and having a proven record of respecting the company rules and policies via agreements and even extenuating circumstances agreements, as could be the case during an unexpected pandemic for example where all employees had no choice but to telework. These agreements should be signed during the onboarding process.

When a new employee joins the organization, they get enrolled into an indoctrination course. This is an orientation course that combines a set of rules and a clear explanation of the organization's culture and its commitments to excellence and perfection. This new layer could be called "The Indoctrination Layer".

The proposed modified BYOD Policy Framework is shown below.



XIV. BYOD VS REMOTE ACCESS

Although the two terms may seem interchangeable, BYOD and remote access are not the same. The word "bring" your own device suggests the user is bringing his device to work, but lately with the COVID 19 Challenges, Users have been staying at home. So, it is more accurate to relate to their work model as a remote access rather than a BYOD access. Regardless of the type of access, both BYOD and remote access present crucial challenges to overcome.

Multiple factors are to be considered such as:

- Organization information security strategy: top-down or bottom up?
- Leadership support to the CISO strategic planning, agile or solely predictive
- Governance and human resources, flexibility, or rigidity.
- Policies and regulations enforcement.
- End Point security, private device security, BYOD security, Security as a service (SAS).
- End user awareness and training.

Many strategies have been implemented to move the U.S. Government towards Zero Trust Cybersecurity Principles as an effort to comply with the directives of the Executive Order 14028 "Improving the Nation's Security" [47]; such as the Office of Managements and Budget's (OMB) "Federal Zero Trust Strategy" [48], the Cybersecurity and Infrastructure Security Agency (CISA) developed "Zero Trust Maturity Model" [49], and the CISA Cloud Security "Technical Reference Architecture" (TRA) [50], This new adaptability mindset clearly explained in the executive order 14028 in the next paragraph, dictates the importance of the mentioned stakeholders in adapting and finding new ways to maintain the national security protected. The current business continuity challenges facing the nation coming out of a multiple years pandemic makes this clause all too valuable and ease the inherent vulnerabilities of BYOD or, as some call "bring your own danger" [51]

XV. NIST IMPACT ON REMOTE ACCESS

Organizational leaders can embrace the NIST cybersecurity framework [52] as a guide in addressing the new workforce challenges of managing remote access for a large volume of employees. The following steps represent the necessary actions that may be taken to assess and triage the organizations cybersecurity infrastructure and adapt its security posture to address the emerging risks of remote access.

1. Triage and prioritize immediate action: When a key executive such as a Chief Information Security Officers (CISO) exits an organization, the new CISO should begin their duties by planning and conducting an assessment of the organizations state of cybersecurity. The NIST Cybersecurity Framework can serve as a useful structure for this assessment. To begin the assessment, a team of organizational subject matter experts should be assembled to include representatives from the current cyber security team, information technology and network administration team as well as human resources and physical security. The initial assessment should identify the highest risks areas and triage any significant risk exposures such as terminating user accounts for employees that are no longer associated with the organization, updating system patches and forcing password changes where appropriate. The goal of this phase is to produce a high level – critical risk score card, identify the most significant risk exposure and take immediate action to remediate significant risk exposure.

2. Establish a steering committee:

At the completion of the initial risk assessment and with the mitigation of significant risks, the CISO can then begin to look at the long-term sustainability of their overall cybersecurity program. The establishment of a steering committee can help to assure that a cross function team of subject matter experts and key stakeholders is

assembled and have a voice in providing strategic guidance to the organization's cybersecurity program. Potential steering committee members could include representatives of operations, finance, human resources, and information technology. The steering committee should be created with a written charter and have scheduled routine meetings.

3. Conduct an extensive risk assessment and IT Asset Inventory: Once established, the steering committee can oversee the creation of an IT asset inventory, the conduct of a penetration test and vulnerability assessment and a complete risk assessment producing the organizations baseline assessment. This baseline assessment will include the core elements of the NIST Cybersecurity framework to Identify, Protect, Detect, and Respond and Recover [52]. The CSC Top 20 controls will also be referenced as part of the organizations assessment of internal controls [40]. Once risk has been inventoried and prioritized long term mitigation strategies can be implemented and an inventory of critical cybersecurity controls can be created and added to the organizations internal audit process to assure sustainability of the cybersecurity program.

4. Develop a prioritized risk mitigation plan: The process of risk management is to inventory existing risk, manage current risk and serve as a platform for the assessment of risk as the organization changes. The effective prioritization of risk helps assure prudent financial management and aids in the cost/benefit analysis needed to support cybersecurity investment. CISO's should select a risk management tool to support the risk assessment process. The Failure Modes Effects Analysis (FMEA) [53] spreadsheet is a tool that can be used as the organizations risk register and will serve as the central location of documented risks, their ranking based on their level of impact on the organization, their probability of occurrence, and the strength/weakness of existing controls. Risks will be prioritized for action based on a plan for 90-day remediation of high impact risks and 180-day remediation for moderate risk. The use of a risk register tool will support the long-term sustainability of the organization's cybersecurity program.

With the risk assessment process complete the time for "plan execution" begins the "Plan Do Check Adjust" (PDCA) cycle is a useful model for CISO's to consider. A team-based approach should also be considered to help divide the work into different operational units. Organizational support will be facilitated through the use of the cybersecurity steering committee. Risk mitigation will be managed in terms of a 90-day plan to address the risks with the highest risk priority number. The Chief Information Officer will serve as the primary executive sponsor to provide for decision-making and budgetary approvals. A process for continuous improvement will be implemented for ongoing improvements to include a review of all policies and procedures, service level agreements and procurement of cybersecurity technologies.

XVI. COVID BUSINESS CONTINUITY PLANNING

The COVID business continuity planning is strategy federal and civilian agencies are drafting and implementing to maintain all functional areas operational as the organization is transitioning back to normal business operations. Organizations are assessing the benefits and drawbacks of BYOD, teleworking, and remote access solutions. It has been challenging for information security executives to weigh in the new mindsets of distributed workplaces, and virtual teams' IT asset and connectivity structures.

The information security challenges presented by the ever-evolving devices and connectivity make endpoint security the most challenging factor to the organization information security. The Cybersecurity Infrastructure Security Agency leads the national efforts to defend critical infrastructure against threats of today and tomorrow [54]. In collaboration with government and civilian entities CISA has several tools and methodologies that can help organizations increase their cyber security posture such as:

- The CISA continuous diagnostics and mitigation (CDM) Program which has tools such as govCAR , DoDCAR where "CAR" stands for Cybersecurity Architecture Review [55]
- TIC 3.0: Trusted Internet Connections 3.0 [56].
- EINSTEIN: which is a system that identifies common baselines of security and help agencies manage their cyber risk [57].

- Using Self Assessments such as the Cyber Resilience Review (CRR) from CISA [58].
- Using toolkits and guides such as CISA cybersecurity awareness program toolkit [59]
- Using the CISA Cyber Essentials [54].

The Zero-trust strategy is a central piece in the post COVID cybersecurity mindset [47]-[48]. Especially where Government agencies are adopting it as an important strategy as stated in the NIST SP 800-207 outlining the zero-trust architecture NIST suggests [60].

XVII. CONCLUSION

The COVID-19 pandemic has changed the world in many ways, and the management of security concerns on corporate networks was one of the first paradigms to shift. The Covid-19 stay-at-home orders resulted in many employees shifting their traditional form of work in an office environment to a work-from-home, remote telecommuter model. Almost overnight, the CISOs had seen their network security risk expand significantly beyond their protected perimeter and move into the homes of each of their employees. which may cause breaches and lead to fraudulent activities as stated in [61]. the challenge to managers working from home became even more daunting as implied in [62]. This change resulted in a need to define a new computing paradigm, to redefine Bring Your Own Device Polices and to provide new end-point protection and virtual private network models. In this new, remote work paradigm, how would CISOs maintain information technology asset management programs, how would they secure all endpoints and network connections, how would they assure authentication was valid and how would they train their end users to be aware of social engineering attacks that may reach them in their homes? Securing devices was not the only concern that increased but also the ability to provide for the privacy and confidentiality of information that was once processed in corporate cubicles and was not flowing across employee's home networks. In addition, these new challenges caused the role of the CISO to be redefined and organizations demonstrated significant variation in how the level of authority and scale of responsibility was imparted onto those serving in their CISO role.

No C-suite role in the history of American business has had such impact on national security as the role of the Chief Information Security Officer in securing their organization from cyberattack and contributing to the protection of US national critical infrastructure. The National Institute of Standards and Technology provides the NIST Cybersecurity Framework, SP800-53 Security and Privacy for Federal Information Systems and Organizations [63] and the NIST National Initiative for Cybersecurity Education framework or commonly known as "NICE Framework" [64]. Given the importance of the CISO role in protecting American business and critical infrastructure, should NIST create a standard that more clearly defines the CISO job duties? Perhaps one of the lessons learned from the corporate response to the pandemic is the need for a standards organization to more clearly outline the role and duties of the CISO to support the CISO's effectiveness in securing the enterprise and critical infrastructure to align with the Executive order 13636 "Improving Critical Infrastructure Cybersecurity" and the Framework for Improving Critical Infrastructure Cybersecurity [65].

As we consider these past challenges and look toward the future, it is apparent that privately held organizations and government institutions must become flexible and change quickly to adapt to new challenges. It will also follow that the role of the Chief Security Executive will adapt as well with new responsibilities being defined and a new scope of authority provided to meet emerging challenges.

REFERENCES

[1] Tallyfy, Inc., "Policy management: What is it and why is it important?", (n. d.) . [Online]. Available: https://tallyfy.com/policy-management/

[2] D. Drew, "Before the Coronavirus, Telework was an optional benefit for the affluent few", March 2020. [Online]. Available: Pew Research Center: https://www.pewresearch.org/fact-tank/2020/03/20/before-the-coronavirus-telework-was-an-optional-benefit-mostly-for-the-affluent-few/

[3] T. Walsh, "The 10 security domains". 2012. [Online]. Available: AHIMA Practice Brief: http://www.advancedmedrec.com/images/The10SecurityDomains.pdf

[4] A. Elgbouri, and S. Mensch, "Factors affecting information security and the widest implementations of bring your own device (BYOD) programs", 2020. [Online]. Available: https://acet.ecs.baylor.edu/journal/ACETJournal_Vol14/BYOD%20Programs_with%20Dr.%20El%20Gbouri%20and%20Mensch.pdf

[5] A. D. Veiga, and J. H. P. Eloff, "An information security governance framework. Information Systems Management", vol. 24, no. 4, pp. 361-372, 2007. [Online]. Available https://doi.org/10.1080/10580530701586136

[6] National Security Agency, "Threat intelligence and assessments", n. d., [Online]. Available: https://www.nsa.gov/What-We-Do/Cybersecurity/Threat-Intelligence-Assessments/

[7] J. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present. Third International Workshop on Cyberspace Safety and Security (CSS)", pp. 21-26, 2011. [Online]. Available: https://ieeexplore.ieee.org/document/6058566

[8] D. Shackleford, "SANS 2019 cloud security survey", 2019. [Online]. Available:https://www.sans.org/reading-room/whitepapers/analyst/2019-cloud-security-survey-38940

[9] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf, and L. Buckalew, L., "BYOD: A global perspective, harnessing employee-led innovation", 2013. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf

[10] M. Colon, "Embracing BYOD". SC Magazine: vol. 23, no. 8, pp. 26-27, 2012.

[11] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir and E. H. M. Saad, "BYOD: Current state and security challenges," 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014, pp. 189-192, doi: 10.1109/ISCAIE.2014.7010235.

[12] C. Middleton, "Mobile media and next-generation broadband: Policy and markets". In G. Goggin & L. Hjorth (Eds.), The Routledge companion to mobile media, pp. 94-103, 2014. New York and London: Routledge

[13] Intersoft Consulting. "General data protection regulation (GDPR): International cooperation for the protection of personal data", n. d., [Online]. Available: https://gdpr-info.eu/art-50-gdpr/

[14] D. Tran, "The law of attribution: Rules for attributing the source of a cyber-attack". Yale Journal of Law and Technology, vol. 20, no. 1, pp. 376-4410, 2018.

[15] G. Gökçe, and O. Dogerlioglu, "Bring your own device policies: Perspectives of both employees and organizations. Knowledge Management & E-Learning", vol. 11, no. 2, pp. 233-246, 2019. https://www.kmel-journal.org/ojs/index.php/online-publication/article/view/411

[16] K. Madzima, M. Moyo, and H. Abdullah, "Is bring your own device an institutional information security risk for small-scale business organisations?", 2014 Information Security for South Africa (IEEE), 2014, pp. 1-8.

[17] L. DeShield, "The challenges of implementing bring your own device", 2017. [Online]. Available: https://pdfs.semanticscholar.org/72ad/2e8689233676c065819204b88d34515fd3a2.pdf

[18] M. D. Kiernan, "Legal ethics and concerns with security in a bring your own device program", Issues in Information Systems, vol. 17, no. 4, pp. 254-259, 2016.

[19] S. Preibusch, "Privacy behaviors after Snowden", Communications of the ACM, vol. 58, no. 5, pp. 48-55, 2015. https://doi.org/10.1145/2663341

[20] B. H. Jones, A. G. Chin, and P. Aiken, "Risky business: Students and smartphones", TechTrends, vol. 58, no. 6, pp. 73-83, 2014. https://doi.org/10.1007/s11528-014-0806-x

[21] B. Boynton, "Identification of process improvement methodologies with application in information security", Proceedings of the 4th annual conference on Information security curriculum development (InfoSecCD '07). 2007, ACM, New York, NY, USA, Article 28. https://doi.org/10.1145/1409908.1409939

[22] P. Bannerman, "Capturing business benefits from process improvement: four fallacies and what to do about them", Proceedings of the 1st International Workshop on Business Impact of Process Improvements (BiPi '08). 2008, ACM, New York, NY, USA, pp. 1-8. https://doi.org/10.1145/1370837.1370839

[23] S. Koffer, L. Anlauf, K. Ortbach, and B. Niehaves, "The intensified blurring of boundaries between work and private life through IT consumerization", Proceeding of the European Conference on Information Systems (ECIS 2015), 2015. 108. doi:10.18151/7217396. [Online]. Available: https://aisel.aisnet.org/ecis2015_cr/108/

[24] S. Haag, and A. Eckhardt, "Shadow IT. Business & Information Systems Engineering", vol. 59, no. 6, pp. 469-473. 2017, https://doi.org/10.1007/s12599-017-0497-x

[25] A. Ekert, and R. Renner, "The ultimate physical limits of privacy", Nature, vol. 507, pp. 443-7, 2014. https://doi.org/10.1038/nature13132

[26] K. McGuire, "Critical factors affecting 'bring your own device' security incidents through security awareness training", 2017, [Online]. Available: https://fairfax.instructure.com/courses/81/files/7596?module_item_id=10402

[27] D. Adams, B. Ives, and I. Junglas,, "Tactical NAV: Innovation in the US Army", Journal of Information Technology Teaching Cases, vol. 8, pp. 1-8, 2012. https://doi.org/10.1057/jittc.2012.5

[28] B. Niehaves, S., Köffer, and K. Ortbach, (2013), "IT consumerization under more difficult conditions: Insights from German local governments", Proceedings of the 14th Annual International Conference on Digital Government Research (dg.o '13). 2013. ACM, New York, NY, USA, pp. 205-213 https://doi.org/10.1145/2479724.2479754

[29] Nokia Corporation, "Nokia threat intelligence report – 2019", 2019, [Online]. Available: https://onestore.nokia.com/asset/205835?did=d0000000016z&utm_campaign=threatintelligence18&utm_source=marketo&utm_medium=LandingPage&utm_content=report&utm_term=awareness

[30] H. Alimardani, and M. Nazeh, "A taxonomy on recent mobile malware: Features, analysis Methods, and Detection Techniques", In Proceedings of the 2018 International Conference on E-business and Mobile Commerce (ICEMC '18). 2018, ACM, New York, NY, USA, pp. 44-49. https://doi.org/10.1145/3230467.3230478

[31] A. Garba, D. Murray, and J. Armarego, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments", Journal of Information and Computer Security, 2017, vol. 25, no. 4, pp. 475-492. https://doi.org/10.1108/ICS-03-2016-0025.

[32] L. Weber, and R. J. Rudman, "Addressing the incremental risks associated with adopting bring your own device", Journal of Economic and Financial Sciences, 2018, vol. 11, no. 1.

[33] G. Gheorghe, and S. Neuhaus, "Preserving privacy and security for personal devices", CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer Communications Security, 2013, pp. 1359-1362. https://doi.org/10.1145/2508859.2512500

[34] J. Oltsik, "ESG: a multitude of mobile security issues. Network World", 2012, [Online]. Available: http://www.networkworld.com/article/2222813/cisco-subnet/a-multitude-of-mobile-security-issues.html

[35] S. Gittlen, (2012, April 2). "Sample of BYOD user policies. Network World", April 2012. [Online]. Available: https://www.networkworld.com/article/2187223/a-sampling-of-byod-user-policies.html

[36] USMC C4/CIO, "Marine Corps mobile device strategy", 2013, [Online]. Available: https://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/USMC_Commercial_Mobile_Device_Strategy_Comm_Paper_04.24.13.pdf

[37] United States Department of Defense, "Telework policy: Instruction 1035.01", 2012, [Online]. Available: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/USDODi/103501p.pdf

[38] T. Stagliano, A. DiPoalo, and P. Coonelly, P., "The consumerization of information technology", Graduate Annual, vol. 1, no. 1, [Online]. Available: https://digitalcommons.lasalle.edu/graduateannual/vol1/iss1/10

[39] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, (2017). "Organizational information security policies: A review and research framework", European Journal of Information Systems, 2017,vol. 26, no. 6, pp. 605-641. https://doi.org/10.1057/s41303-017-0059-9

[40] A. Hovav, and F. Putri, "Employees´ compliance with BYOD Security policy: Insights from reactance, organizational justice, and protection motivation theory", Association for information systems, AIS electronic library. European Conference on Information Systems ECIS 2014 proceedings, vol. 9. 2014, [Online]. Available: https://pdfs.semanticscholar.org/e1ff/a26f0ae414f64f508b5d6a333a58d0564b6e.pdf

[41] O. C. Ekwuabu, "Improving systems design and implementation: An examination of the effect of good requirements definition on end-user satisfaction." Capella University, 2007.

[42] J. D'Arcy, T. Herath, and M. Shoss, (2014) "Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems", vol. 31, no. 2, pp. 285-318, 2014. https://doi.org/10.2753/MIS0742-1222310210

[43] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory". Computers and Security, vol. 31, no. 1, pp. 83-95, 2012. https://doi.org/10.1016/j.cose.2011.10.007

[44] H. Rhee, Y. Ryu, and C. Kim, (2102) "Unrealistic optimism on information security management". Computers and Security, vol. 31, pp. 221-232. 2012. https://doi.org/ 10.1016/j.cose.2011.12.001.

[45] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity [PowerPoint Presentation]. 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/Cybersecurity-Framework-Overview/images-media/NIST%20CSF%20Overview.pdf

[46] V. Venkatesh, J. Thong, & X. Xu, (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems*, 175, pp. 328-376.

[47] White House Executive Order 14028, "Improving the Nation's Security". May 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[48] Executive Office of the President, Office of Management and Budget, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles". January 2022. [Online] Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[49] Cybersecurity and Infrastructure Security Agency (CISA), "Zero Trust Maturity Model". June 2021. [Online]. Available: https://zerotrust.cyber.gov/zero-trust-maturity-model/

[50] Cybersecurity and Infrastructure Security Agency (CISA), "Cloud Security Technical Reference Architecture (TRA)". August, 2021. [Online]. Available: https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/

[51] Ali MI, Kaur S. Next-generation digital forensic readiness BYOD framework. Security and Communication Networks. 2021 Mar 22;2021.

[52] National Institute of Standards and Technology, "NIST cybersecurity framework: New framework". April 2022. [Online]. Available: https://www.nist.gov/cyberframework/getting-started#background

[53] Failure Mode Affect Analysis Tool, "Guidance for Performing Failure Mode and Effects Analysis with Performance Improvement Projects", [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiqwqnny-r5AhVCkmoFHcl3DjAQFnoECE8QAQ&url=https%3A%2F%2Fwww.cms.gov%2FMedicare%2FProvider-Enrollment-and-Certification%2FQAPI%2Fdownloads%2FGuidanceForFMEA.pdf&usg=AOvVaw26ZXBEexo3aDNmZyRp7RQD

[54] Cyber security and infrastructure security agency, "CISA Cyber Essentials", 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

[55] Cyber security and infrastructure security agency, "Continuous Diagnostics and Mitigation (CDM) Program", 2012, [Online]. Available: https://www.cisa.gov/cdm

[56] Cyber security and infrastructure security agency, "TIC 3.0: Trusted Internet Connections 3.0". (n.d.). [Online]. Available: https://www.cisa.gov/publication/tic-30-core-guidance-documents

[57] Cyber security and infrastructure security agency, "EINSTEIN". (n.d.). [Online]. Available: https://www.cisa.gov/einstein

[58] Cyber security and infrastructure security agency, "Cyber Resilience Review (CRR)". 2016. [Online]. Available: https://www.cisa.gov/uscert/resources/assessments

[59] Cyber security and infrastructure security agency, "CISA Cybersecurity awareness program toolkit". (n.d.). [Online]. Available: https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-toolkit

[60] National Institute of Standards and Technology, "NIST SP 800-207, Zero Trust Architecture". 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[61] Aguboshim FC, Udobi JI. Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD). Information Technology (IT). 2019;8(1).

[62] Kirchner K, Ipsen C, Hansen JP. COVID-19 leadership challenges in knowledge work. Knowledge Management Research & Practice. 2021 Oct 2;19(4):493-500.

[63] National Institute of Standards and Technology, "NIST Privacy and Cybersecurity Framework". September 2020. [Online]. Available: NIST.gov: https://doi.org/10.6028/NIST.SP.800-53r5

[64] National Institute of Standards and Technology, "NICE Framework", 2022. [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework

[65] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity". 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02122014.pdf

Authors: Dr. EL Gbouri has a dual major bachelor's degree in business administration management and information systems management, a Master of Science degree in cybersecurity (2016), and a Doctorate in information assurance (2020).

Dr. El Gbouri works for the United States Navy Medicine as the Department Manager for the Reserve Policy and Integration, Manpower Systems. He also currently occupies the position of faculty in the Computer Science and Cybersecurity Department at Laurel Ridge Community College. The work of Dr. El Gbouri spans from high visibility project management of efforts of national impact to policy drafting for process improvements, design, and engineering. The scope of his work includes multiple disciplines, from systems, to education, training and planning and operations.

Dr. El Gbouri is a member of the United States Navy, he holds several military awards including a Navy and Marine Corps Commendation Medal, and seven Navy and Marine Corps Achievement Medals.

abdessamad.elgbouri@gmail.com

Dr. Scott Mensch's areas of expertise are in network security and business/project management. Shortly after graduating with a bachelor's degree and obtaining a position with an engineering firm, furthering his education was imperative. He completed his M.B.A. in 1998 and obtained two additional associate degrees in computer applications and networking in 1999. In 2007 he completed his Ph.D. in organizational management with a Specialization in IT along with post-doctoral studies in advanced telecommunications.

Dr. Mensch began working in education in 2001 while teaching at a community college. He has taught and developed programs in Business and IT for the past 21 years both online and in a face-to-face modality. He currently teaches graduate IT classes at Purdue Global University.

Dr. Mensch is a member of IEEE, and sits on several strategic planning committees.

scott.mensch@purdueglobal.edu

Mr. Michael Pry's area of expertise is in the area of risk management and cybersecurity. Maintaining a blend in his skill set between the investigative and risk focused discipline of criminal justice and the technological components of information systems, he has supported the risk management efforts of multiple organizations in multiple industries for over 20 years since completion of his undergraduate degree. Driven by passion for the field, he later pursued a Master's of Science in Computer Science graduating in 2009 and continues to pursue excellence in the field through research and writing.

Mr. Pry is currently pursuing his doctorate degree in computer science with a concentration in cybersecurity and enjoys researching and writing on multiple topics within the cybersecurity field.

Mr. Pry is a member of ISC2, and volunteers his time supporting a variety of community organizations.

Mpry2@outlook.com