Taylor & Francis
Taylor & Francis Group

Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

BYOD security issues: a systematic literature review

Melva Ratchford, Omar El-Gayar, Cherie Noteboom & Yong Wang

To cite this article: Melva Ratchford, Omar El-Gayar, Cherie Noteboom & Yong Wang (2021): BYOD security issues: a systematic literature review, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2021.1923873

To link to this article: https://doi.org/10.1080/19393555.2021.1923873

Published online: 22 Jul 2021.

Submit your article to this journal

Article views: 92

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=uiss20

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2021.1923873

Taylor & Francis
Taylor & Francis Group

Check for updates

BYOD security issues: a systematic literature review

Melva Ratchford, Omar El-Gayar, Cherie Noteboom, and Yong Wang

Dakota State University, Madison, United States

ABSTRACT

Organizations are exposed to new security risks when they allow employees' personal mobile devices to access the network and the corporate data (a phenomenon called 'Bring Your Own Device' or BYOD). They are confronted with inherent security issues that need to be addressed in order to protect the organization and its information. What are the security issues and considerations associated with BYOD environments? With this in mind, the objective of this paper is to present a systematic literature review of scholarly literature (2010–2019) with respect to BYOD security, and to suggest a classification scheme that depicts a holistic approach to securing BYOD environments. The results of this review include the analysis of 38 scholarly articles, where 22 security issues were identified. Based on the proposed classification scheme, the analysis of the findings shows that 86% of the articles identified security issues and considerations associated with the IT domain, 51% identified security issues related to the Management domain, 45% related to the Users domain, and 19% related to the Mobile Device domain. The results also show that BYOD security issues corresponding to policies are among the most frequently addressed concerns, followed by network security, data protection, user's attitude/behavior and governance.

KEYWORDS

BYOD security; byod environments; systematic literature review

1. Introduction

As the use of personal mobile devices, specifically mobile phones and tablets, accessing corporate data continues to grow, a phenomenon known as Bring Your Own Device (BYOD), organizations realize that allowing this type of access reduces cost and increases productivity (Bello Garba et al., 2015). Employees want to operate in a style that allows them to use 'any-device, anywhere,' mixing personal activities with work activities at any time, and making this situation a byproduct of IT consumerization (Ogie, 2016). BYOD is rapidly becoming the norm rather than the exception (Crossler et al., 2014), and, 'whether companies like it or not, this is a trend that is happening' (Absalom, 2012). Organizations need to ensure that the Confidentiality, Integrity and Availability (CIA) of their information is preserved (McCumber, 2004). In addition to corporate data protection, the adoption of BYOD brings other considerations such as protection of private information as well as legal considerations that can negatively affect an organization if not addressed (Utter & Rea, 2015). There is a need to analyze the security of BYOD environments as a whole rather than analysis of isolated areas (Zahadat et al., 2015).

To date, few systematic reviews of BYOD have been performed. These include reviews that discuss BYOD challenges and privacy issues (Oktavia et al., 2016), reviews that focus on the integration of BYOD within the enterprise (Amoud & Roudies, 2017), works that concentrate on BYOD policies tailored to hospital environments (Moyer, 2013), and reviews that discuss BYOD issues specific to other countries (Herrera et al., 2017). However, there is a need for deeper understanding of the BYOD phenomenon that accounts for the multifaceted aspects of BYOD security. Specifically, this literature review extends prior works since, in addition to the identification of BYOD security issues, it includes a classification scheme based on a holistic approach to security, where BYOD security issues are identified and classified based on organizational domains associated with Management, Information Technology (IT), BYOD Users, and personal Mobile Devices. The question this study

CONTACT Melva Ratchford MELVA.RATCHFORD@trojans.dsu.edu Dakota State University, Madison 57042-1799, United States
© 2021 Taylor & Francis Group, LLC

aims to answer is: *What are the security issues and considerations associated with BYOD environments?*

Toward this aim, we propose a classification scheme for security issues in BYOD environments based on extant literature and representing a holistic perspective that accounts for the multi-faceted aspects of BYOD security. We follow the guidelines proposed by Liberati et al. (2009) in their Preferred Reporting Items for Systematic Reviews (PRISMA) in order to identify and discuss BYOD security issues, in accordance with the proposed classification scheme. From a theoretical perspective, the research provides a synopsis into the current state of BYOD security research that provides insights for future research with an emphasis on a holistic multi-faceted perspective. From a practical perspective, the findings could provide guidance to practitioners and organizational decision makers into prevailing issues associated with BYOD security in a holistic multi-faceted manner.

After this introduction, this paper is structured as follows: Section 2 presents a classification scheme for a holistic perspective to BYOD security. Section 3 describes the research method and criteria employed in this review. Section 4 presents its results. Section 5 provides an analysis of the results, suggests future research, and provides concluding remarks.

2. Classification scheme

Enterprise security has been a topic of concern since the development of the Internet. Several frameworks have been proposed in order to provide infrastructure protection to organizations. Among these frameworks, we relied on the Institute for Critical Information Infrastructure Protection (ICIIP) conceptual framework (Kiely & Benzel, 2006) and the McCumber's Cube (McCumber, 2004) as representative frameworks that clearly depict the main concepts associated with securing an organization's information.

'Enterprise security includes all of an organization's aspects' as stated by Kiely and Benzel (2006) and depicted by their ICIIP conceptual framework shown in Figure 1. In it, the authors define elements beyond the traditional people, process and technology by depicting a 3D pyramid that includes elements (and their relationships) necessary to secure systems (Kiely & Benzel, 2006).

In the same manner, McCumber (2004) explains the security of information when associating the critical information characteristics of CIA with the security measures established through technology, policies, and human factors as the information is transmitted, stored or processed as depicted in McCumber's Cube in Figure 2. When protecting BYOD environments, the same security principles apply and another characteristic is added to represent the mobile device, since it is not a device under the control of the organization but rather a device under the control of the employee.

Adopting information security concepts from McCumber (2004) and the ICIIP (Kiely & Benzel, 2006) and adding inherent risks posed by BYOD (e.g., comingle of personal and

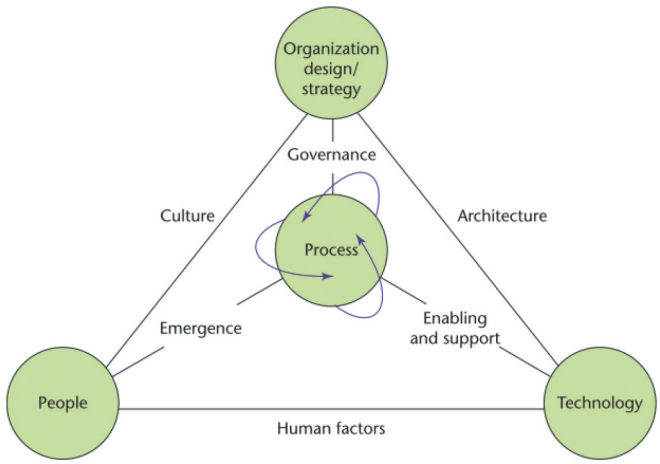

Figure 1. Institute for critical information infrastructure protection (ICIIP) conceptual framework (Kiely & Benzel, 2006).

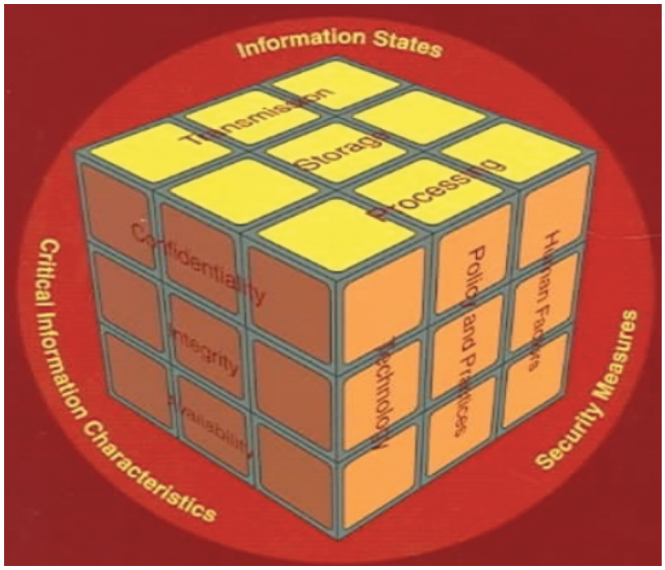

Figure 2. McCumber's cube. security of information (McCumber, 2004).

organizational data, privacy of personal device, legal issues, etc.), this review categorizes the security issues as they relate to the domains of an organization as follows: Management Domain, Information Technology (IT) Domain, User Domain and Mobile Devices Domain. Using a scheme based on a concept-centric approach (Ngai et al., 2011; Webster & Watson, 2002), Figure 3 shows the proposed classification scheme for security issues related to BYOD environments.

Safeguards associated with IT, Management and Users need to be implemented in order to integrate technology, policy management, and people and thus protect BYOD environments (Zahadat et al., 2015). The classification proposed in Figure 3 adds a fourth domain corresponding to Mobile Device since there are physical characteristics required of the devices themselves (e.g., types of operating systems, security capabilities, personal setup, etc.). A description of each of the four domains follows.

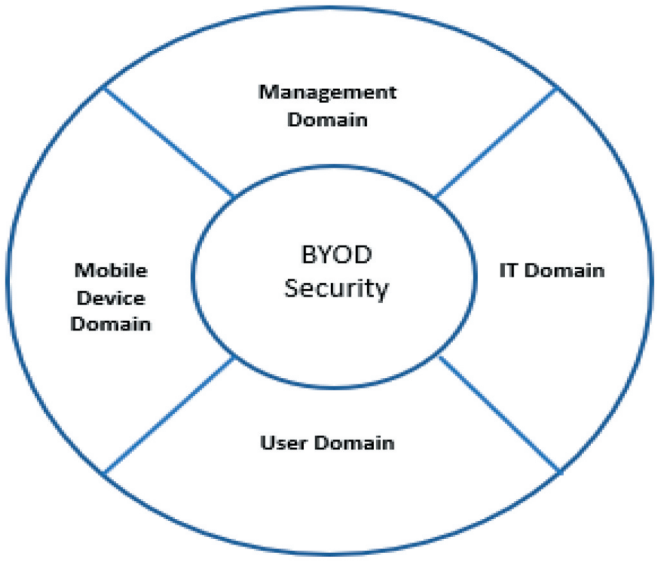

Figure 3. Classification scheme for security issues in BYOD environments.

2.1. Management domain

At the organizational level, there is the need to design structures and strategies to allow the enterprise to compete effectively, to define its risk tolerance, and to create governance practices that elevate security to a top priority level (Kiely & Benzel, 2006). Management needs to adopt a holistic approach to securing the information of an organization. This includes the overseeing of security-related activities such as the development and execution of information security policies, training and awareness program compliance, the development of the organization's information architecture, IT infrastructure and business alignment, and human resources management (Soomro et al., 2016).

The decision to adopt BYOD needs to be made at the executive level of an organization, since governance is critical to the success of BYOD (Thompson, 2012). BYOD should be subject to monitoring and management oversight (ISACA, 2016). Policies need to be determined at the management level, however there are inconsistent security policies across departments, and these discrepancies in security policies are the genesis for most security failures (Zahadat et al., 2015). In addition, security is a corporate governance responsibility and a business issue that needs to be addressed separately from the traditional technical considerations (Von Solms, 2006; Zahadat et al., 2015). With respect to BYOD, Management responsibilities can be categorized/associated with sub-domains such as governance, risk management, training and awareness, legal issues, help desk, policies, and HR, among others (Ratchford & Wang, 2019).

2.2. IT domain

IT represents the domain responsible for developing and implementing the technological approach to protect the organization's information and stay ahead of possible threats that can corrupt the systems (Kiely & Benzel, 2006). IT departments are the enablers of the BYOD environments (Zahadat et al., 2015). The use of these devices for personal and corporate access creates a new set of threats for IT departments (A. Scarfo, 2012). IT is the domain with most security responsibilities associated with implementation of BYOD. It is responsible for planning and minimizing security risks to the network (Hernandez & Choi, 2014). This includes implementation of security controls related to wireless communication, Virtual Private Networks (VPN), cellular technologies, Wi-Fi, Bluetooth, and network monitoring tools.

IT is also responsible for security issues related to third party access, employees access control, data protection, device configuration, cloud access, encryption, anti-malware, patch updates, and mobile device issues such as app control, device detection, jailbreak/root, browser, and password enforcement. IT departments need to provide Helpdesk and user support in order to increase employees' compliance (Hovav & Putri, 2016). In addition, IT plays important security roles in training and awareness programs, policy enforcement, and risk assessments. However, in order to properly implement security controls, there needs to be an IT alignment with the business needs and organizational strategies (i.e., management) in order to reduce security incidents (Soomro et al., 2016).

2.3. User domain

'Humans are the most critical element in information security management' (Soomro et al., 2016). There is a positive effect to information security when the employees are properly trained and are aware of security issues, however, they can act with malicious intent when stealing the organization's information (Soomro et al., 2016). The users represent the people who must 1) practice fundamental security hygiene (i.e. implement security practices and procedures such as strong and frequently changed passwords, separation of duty, etc.) and 2) be properly trained in order to secure the organization's communications and its corporate data since the 'the human factor is vital to managing and perfecting security' (Kiely & Benzel, 2006). When users are allowed to use their personal devices to access the organization's system, the users' perception is influenced by the security controls imposed by the organization (e.g., data encryption, remote wipe, VPN) and the liabilities (e.g., possible job termination, financial impact, loss of privacy) the user may incur, and this perception influences the

user's behavior (Yang et al., 2013). Therefore, the organization needs to ensure the user understands, agrees and signs the relevant policies before connectivity is allowed. Businesses need to be clear with employees in order to avoid confusion and protect the organization against BYOD-related risks (United-Kingdom, 2012).

Other BYOD-related issues that affect users, involve privacy and intrusiveness concerns, especially when personal and corporate data comingle in the same space. The privacy paradox (Gerber et al., 2018) between user's privacy concerns and actual user's behavior needs to be addressed through training, awareness, and policies. Users' concerns also include issues related to mobile device resource consumption associated with agents (or special applications) that need to be installed in the device (by the organization) for device enrollment and monitoring purposes (Wang et al., 2014).

2.4. Mobile device domain

There are several options organizations need to consider before allowing BYODs. These range from complete virtualization to various forms of device control. When considering mobile device security, the goals for a secure BYOD environment are space isolation (separation of personal and corporate data), security policy enforcement, corporate data protection, non-intrusiveness, low-resource consumption, and true space isolation (i.e. corporate data not stored in user's mobile device) (Gimenez et al., 2015). The properties that these goals address are: confidentiality, integrity, availability, authentication, authorization, accountability and privacy (Gimenez et al., 2015). Furthermore, the implementation of security controls that directly affect the mobile device itself involves responsibilities associated across the domains discussed earlier. For example, a device lost or stolen situation involves IT (i.e. IT needs to execute a device wipe), the User (i.e. the user needs to report the loss of the device) and Management (i.e. there needs to be a policy that requires the user to report of the compromised device). There are different solutions available when seeking to manage BYODs. The organization needs to consider these goals and properties when deciding how to manage personally owned mobile devices.

2.5. Security issues

Security concepts are addressed by various ontologies and taxonomies. For example, the ontologies described by ISO/IEC 27001:2013 Standards (27001Academy, 2017b; Disterer, 2013b) and the NIST 800–12 Handbook Introduction to Computer Security (Guttman & Roback, 1995) define assets, threats, vulnerabilities and controls concepts in the context of organization security. Based on the NIST 800–12 ontology, Fenz et al. (2009) proposed a Security Relationships Model that includes the relationship between assets, threats, vulnerabilities and controls and the relationship among themselves. Likewise, the ISO/IEC 27001 standard describes a risk assessment and treatment process based on assets, threats, and vulnerabilities approach (27001Academy, 2017b).

In the context of this research, and drawing from Fenz's Security Relationship Model and the ISO/IEC 27001:2013 standard, the definition for BYOD security issues refers to any type of security concern that represents a threat to organizational assets through the exploitation of a vulnerability, where the implementation of controls is needed in order to mitigate the risks to the organization's assets. In the appendix, Table 1 presents a general explanation of security issues as derived from the following ontologies and taxonomies:

Grundshutz IT Manual and Supplement which is a compilation and definition of elementary threats (Grundshutz, 2004; G. I. Grundshutz)

Basic Concepts and Taxonomy of Dependable Secure Computing which provides definition for basic computer security concepts. (Avizienis et al., 2004b)

Internet Security Glossary which provides information for the Internet community (Shirey, 2000)

National Institute of Standards and Technology Special Publications: 800–12, 800–46, 800–114, 800–125, 800–124, which, in addition to introducing computer security concepts, also define concepts for access control, teleworking, an BYOD security (Guttman & Roback, 1995; Scarfone et al., 2011; M; Souppaya & Scarfone, 2013; Murugiah, 2016a, 2016b)

Common Criteria for Information Technology Security Evaluation which discusses general

Table 1. Security issues related to BYOD – general definition & explanation.

Security Issues & Considerations	Definitions and Explanations
Access Control	Access is the ability to use any system resource. Access controls prescribe not only who or what, but also the type of access that is permitted' (Guttman & Roback, 1995). The ISO 27001 Information Security standards define access controls based on the need: 'To control access to information. To ensure authorized user access and to prevent unauthorized access to information systems. To prevent unauthorized user access, compromise or theft of information and information processing facilities. To prevent unauthorized access to networked services. To prevent unauthorized access to operating systems. To prevent unauthorized access to information held in application systems. To ensure information security when using mobile computing and teleworking facilities. (Disterer, 2013b)
Applications	This refers to controlling what software is used on a system. If users or systems personnel can install and execute any software on a system, the system is more vulnerable to viruses, unexpected software interactions, and software that may subvert or bypass security controls. (Guttman & Roback, 1995)
Best Practices	A proven activity or process that has been successfully used by multiple enterprises (ISACA, 2019b)
Cloud Access	In general, this refers to a 'convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction' (ISACA, 2019a). In terms of BYOD, NIST 800–124 Special Publication discusses this security issue in terms of mobile devices accessing storage resources outside of the control of the organization (Souppaya & Scarfone, 2013).
Compliance	The ISO 27001 standard discusses compliance in term of controls necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. To ensure compliance of systems with organizational security policies and standards. To maximize the effectiveness of and to minimize interference to/from the information systems audit process. (Disterer, 2013b). Compliance can also be defined as ' the adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies' (ISACA, 2019b).
Corporate Data Protection	This refers to the attributes that characterize the security of the organization's information. Avizienis et al (Avizienis et al., 2004b) define these security attributes as confidentiality, integrity, availability, reliability and safety of the information, where confidentiality refers to the 'absence of unauthorized disclosure of information; integrity refers to the absence of improper system alterations'; availability refers to the 'readiness for correct service'; reliability refers to the 'continuity of correct service'; and safety refers to the 'absence of catastrophic consequences on the user(s) and the environment (Avizienis et al., 2004b).
Education	Security awareness, training and education where support and operations staff, as well as users, are trained in security procedures and aware of the importance of security. (Guttman & Roback, 1995)
Employee Behavior/ Attitude	Human-made faults can be non-malicious or malicious. Non-malicious actions can be non-deliberate (i.e. a mistake) or deliberate (i.e. a bad decision) where either action can be accidental or due to incompetence. A malicious fault is a deliberate action. (Algirdas Avizienis, Jean-Calude Laprie, Brian Randell, & Carl Landwehr, 2004b).
IT consumerization	Refers to new trends/modality 'in which emerging technologies are first embraced by the consumer market and later spread to the business' (ISACA, 2019b).
Legal	This refers to legal issues associated with regulatory and contractual compliance (ISACA, 2019a)
Malware	Malware is malicious software developed with the aim of performing unwanted and often harmful operations (Grundshutz, 2004)
Mobile Device Security	A mobile device can be defined as a small device, with at least one wireless network interface, non-removable data storage, where applications are available through multiple methods (Souppaya & Scarfone, 2013). A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds (ISACA, 2019a). In terms of BYOD, mobile device security includes the method through which the organization manages the personally-owned mobile devices and controls the corporate information accessed through the device.
Monitoring	Information Monitoring refers to the 'maintenance of ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions' (Guttman & Roback, 1995). In the context of BYOD, networks that allow BYOD should be monitored in a manner consistent with how remote access segments are secured and monitored (Souppaya & Scarfone, 2016a)
Network	A network is a 'collection of host computers together with the subnetwork or internetwork through which they can exchange data' (Shirey, 2000). For the purpose of BYOD, this issue refers to the connectivity and access of the organization's network, defined as a separate, external dedicated network (e.g., off the organization's DMZ). (Souppaya & Scarfone, 2016a)
Policies	In the context of information security, NIST 800–12 defines policy as an 'aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects, and distributes information' (Guttman & Roback, 1995).
User Privacy	In the context of an individual's privacy, this refers to 'The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed' (Shirey, 2000). An abuse of personal data takes place if an institution collects, for example, too much personal data, collects it without legal basis or consent, uses it for purposes different from the objective stated at the time of collecting, deletes personal data too late or discloses such data in an unauthorized manner.(Grundshutz, 2004)
Risk Management	NIST 800–12 defines risk management within the context of information security as the 'process of minimizing risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation resulting from the operation of a system. (Guttman & Roback, 1995). This also ' entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. (ISACA, 2019b)
Security Management	This refers to the process of establishing and maintaining security for a computer or network system, where the stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution. In network management, the stages are: controlling access to the network and resources, finding intrusions, identifying entry points for intruders and repairing or otherwise closing those avenues of access.(ISACA, 2019b)
Separation of data	This is an issue inherent of BOYD, and it refers to the 'separation of personal space and corporate space on a BYOD' (Yong Wang, Jinpeng Wei, & Karthik Vangury, 2014)
Governance	Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives (ISACA, 2019a)
Virtualization	NIST 800–125 defines virtualization as the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM) (Scarfone et al., 2011)
Helpdesk/User Support	User support takes place through a service desk that can support the entire organization (Guttman & Roback, 1995)

concepts and principles of IT (CCMB- 2012-09-001, 2012).

ISACA Cybersecurity Fundamentals Glossary which defines concepts related to computer security (ISACA, 2019a, 2019b)

ISO/IEC 27001:2013 standard for information security management which discusses IT security issues in general and the applicability to BYOD (27001Academy, 2017a, 2017b; Disterer, 2013a)

3. Methods

3.1. Research method

This systematic review adopts a 3-phase methodological framework proposed by Ngai et al. (2011) where the research approach involves a research definition phase, a research methodology phase, and a research analysis phase.

Phase 1: Research Definition. During this phase, the research area and the research goals are stated. For this research, the area of interest is BYOD security with the research goals and objectives as stated in section 1.

Phase 2: Research Methodology. During this phase, the research scope and research criteria are defined. The scope of this research is limited to the search of online academic scholarly sources in the following databases: Business Source Premier, ABI/INFORM, IEEE Explorer, and Science Direct. The databases were selected because they represent a mixture of business and computer-focused research. The search criteria involve security-based topics and security issues associated with BYOD environments. To ensure that only papers that are specifically focused and relevant to BYOD security-related issues, the search was emphasized the presence of relevant keywords in the title. For this, the following search parameters have been adopted:

Keywords (in title): (security AND (byod OR "bring your own device"))

Scholarly sources with full text availability

Articles time-frame: 2010–2019

Articles written in English

Phase 3: Research Analysis. During this phase, the selected papers are analyzed, and the results are discussed.

3.2. Inclusion and exclusion criteria

The filtering process follows a three-step technique as proposed by Oktavia et al. (2016) where the articles undergo a filtering process categorized as articles found (first round), articles candidate (second round), followed by articles selected (third round). For the purpose of this research, these three steps are defined as follows:

Articles Found: These papers meet the initial search criteria as defined in the parameters delineated in Phase 2 above.

Articles Candidate: The articles undergo further scrutiny. For this research, the abstract, the keywords, and the title are examined. Articles considered as candidates are articles where the *abstract* and the *title* address the research question (RQ). A criterion for paper selection is also based on the question: 'With respect to BYOD, what security issue is the article specifically addressing?' During this stage, duplicate articles, and articles where the abstract does not clearly state the purpose/objective of the paper are eliminated. Articles that are not peer-reviewed are also eliminated (part of the search criteria). Also excluded are papers that refer to systematic reviews, research agendas, and non-academic articles (e.g., whitepapers), as well as papers that do not specifically deal with security issues related to BYOD. Since only scholarly sources and peer reviewed articles are selected, by default this eliminates articles from industry magazines or sources that lack methodological rigor.

Articles Selected: These articles undergo a full-text review and constitute works that specifically address BYOD security issues. For example, specific BYOD issues discussed in the selected articles may include network vulnerabilities, access control protection such as specific discussion of authorization and authentication, discussion of upper management decisions such as BYOD risk acceptance and resource allocation, BYOD users and legal concerns such as protection of privacy and device resource consumption, and other security issues regarding the mobile device itself such as stolen devices, wipe option, and comingled data, among others. The classification of articles based on the security issues identified as part of the classification scheme was

performed by one author and validated by another. If needed, the researchers would discuss any issues to reach a consensus. The document has been revised accordingly.

4. Results

A total of 38 articles were selected after eliminating articles that did not meet the selection criteria, as discussed in section 3. Following PRISMA's flow diagram concepts (Liberati et al., 2009), Figure 4 below summarizes the study selection.

The distribution of articles by year shown in Figure 5, shows that the BYOD phenomenon has been on the rise creating security concerns since 2012. It is interesting to note that, although the time-frame for the search was 2010–2019, the lack of scholarly and peer-reviewed articles prior to 2012 suggests the security concerns probably started shortly before 2012.

In the Appendix: 1) Table 1 lists the definitions of the security issues. 2) Table 2 presents a list of security issues found in the reviewed articles, where the issues have been associated with the article/author's keywords – as shown in the second column. 3) Table 3 presents an analysis of each article. The security issues were extracted and classified based on the proposed classification scheme (domains) shown in Figure 3 and discussed in section 2. Figure 6 shows the articles' distribution based on the findings by domain as follows:

Security issues associated to Management domain = 19 articles

Security issues associated to IT domain = 32 articles

Security issues associated to User domain = 17

Security issues associated to Mobile Device domain = 7

Table 4 displays the concentration of articles per security issue. Analysis of these findings is discussed in the next section. Although a total of 22 security issues were identified, it is interesting to note the concentration of articles based on security issues. It can be noted that the policies associated with BYOD are the most frequently discussed security concerns, followed by network security, corporate data protection, user behavior/attitude, and governance.

5. Discussion

5.1. Analysis

Security concerns with respect to BYOD have been a scholarly discussion since 2012, as depicted by results in Figure 5. The upward trend may be attributed to the increasing number of employees accessing corporate data from their personally owned devices, and the increasing number of organizations that embrace this phenomenon. Based on the classification scheme presented in section 2, the results in Figure 6 and the totals in Table 2 show 86% of security concerns associated with the IT Domain, 51% related to the Management Domain, 45% User Domain related issues and 19% Mobile Device Domain. This indicates that, while technical security issues are the responsibility of the IT departments, there is significant security discussion around the responsibilities associated with management and the BYOD user. In addition, the analysis of each article and its relationship to the classification domains (i.e. Management, IT, Users, Mobile Device), as depicted in Table 3, shows that most of the literature identifies security issues associated with more than one domain, and each domain is concerned with multiple security issues (i.e. a many-to-many relationship). This indicates that, when securing BYOD environments, there is sharing of responsibilities across domains as discussed in many articles. For example, in Table 3, the articles written by Scarfo (2012), Ocano et al. (2015), Downer and Bhattacharya (2015), and Ali et al. (2015) discuss BYOD security issues that are related to all domains. Within the context of a holistic approach to security as proposed in the classification scheme, and upon closer analysis of the findings presented in Table 3, prevailing security issues can be identified for each domain. In this regard, for the Management domain, the literature reveals frequent issues associated with governance, policies, and risk management. For the IT domain, issues related to network, policies, risk management and the implementation of best practices are often discussed. For the User domain, issues regarding users' compliance, attitude/behavior, and privacy take precedence. For the Mobile Device domain, the prevailing issues are associated with device security in general, separation of data and malware.

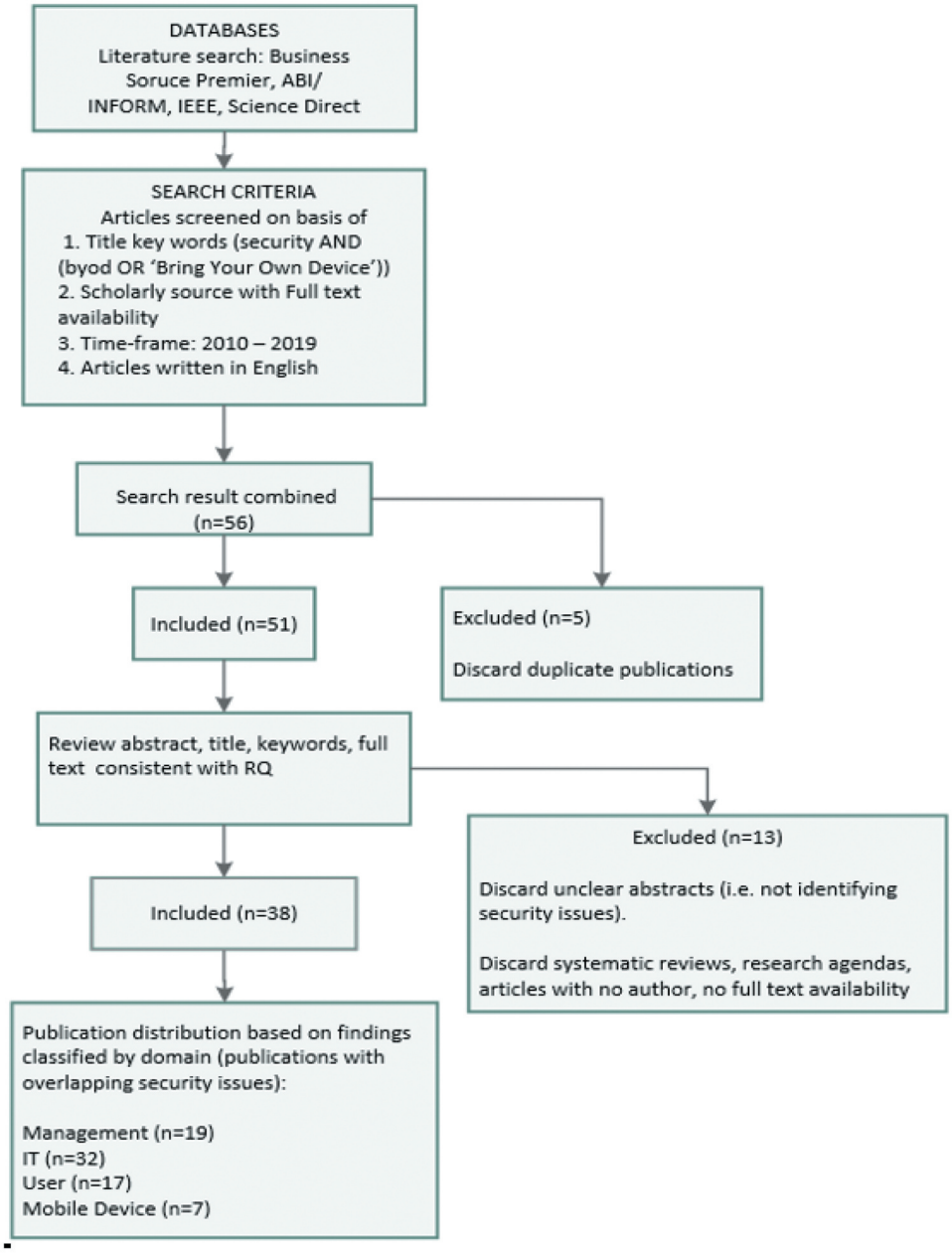

Figure 4. Flow diagram of study selection.

When considering the 22 security issues identified in this study, Table 4 and Figure 7 provide information with regard to the issues that are more frequently addressed. For example, the discussion of policies associated with BYOD has the highest concentration of articles. This may be attributed to the fact that security associated with BYOD involves the enforcement of policies by management (e.g., through HR), the input from IT when including technical aspects in the policies (e.g., prohibition of device jailbreak), and the assurance that the BYOD user understands and complies with the policies. As a countermeasure to policy-related issues, Garba et al (Garba, Armarego, Murray et al., 2015) propose policy-based management model that includes the implementation of information security standards and procedures, information privacy principles, information security and privacy technical controls, liabilities, awareness and training program, and BYOD user perception and behavior (Garba, Armarego, Murray et al., 2015).

It can also be noted that other security issues, although less discussed, represent valid concerns.

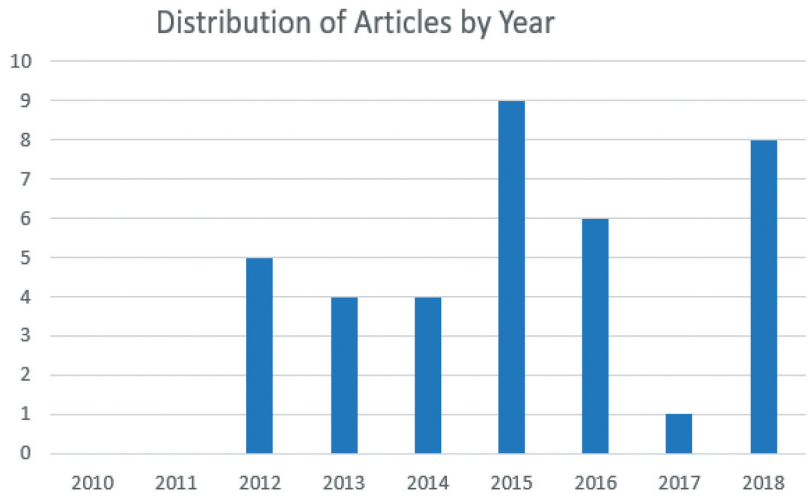

Figure 5. Distribution of articles by year.

For example, the results presented in Table 4 show that topics related to legal considerations are found in one article. In the same manner, other low-count security concerns relate to the separation of data and user support. This does not necessarily indicate that these issues should be discarded, but rather provoke further understanding, especially when considering a holistic approach to security.

The Venn's diagram in Figure 7, shows an overlap of BYOD security issues associated with each of the four domains proposed by the classification in this study. For example, issues associated with Education (e.g., training and awareness) are related to Management, IT and User domains. Although the specific safeguards are different (e.g., Management needs to approve and budget for training/awareness, IT needs to provide technical support, and Users need to take the training), the diagram depicts the necessary symbiosis, across domains, that needs to be part of BYOD security (Ratchford & Wang, 2019).

5.2. Future research

This literature review has identified that IT security issues are well addressed. However, while the IT Domain is dominating the BYOD research field, the User Domain and the Mobile Device Domain issues can benefit from further exploration. Further study of the relationship across domains is needed when considering a holistic approach to securing BYOD environments. How do the four domains overlap in order to ensure a comprehensive approach to BYOD security? Further research could focus on the analysis of this overlap for each issue. As an example of overlap, consider the security issues related to BYOD policies. What are the Management, IT and User's related posture with respect to BYOD policy implementation? Another overlap can be identified in the area of risk management between the IT Domain and the Management Domain. What are the responsibilities of these two domains with respect to risk management/assessment? Deeper understanding is also needed in issues with low article concentration, as identified in Table 4. In addition, this review leaves unanswered the identification of the controls/safeguards associated with each security issue.

The impact of BYOD is fertile ground for further analysis and research aiming to the identification of BYOD security issues. For example, the use of personal 'wearable' devices accessing corporate data, although part of the general BYOD category with respect to information security, may merit research in its own. Other areas suitable for granular BYOD study include e-commerce, m-commerce or mobile-banking, and its impact to the security of organizational information. Another topic of interest for further study could be related to the discussion/comparison of security issues across the different modalities of mobile devices accessing corporate data. These include security issues related to corporate-owned devices vs personally owned

Table 2. BYOD Security issues and considerations as per systematic literature review.

Security Issues	Keywords (provided in the articles)	Articles	No. of Articles
Access Control	Authorization Authentication Access control	(Bann et al., 2015) (Chung et al., 2012) (Ali et al., 2015) (Zheng et al., 2018) (Petrov & Znati, 2018)	5
Applications	Application program Interface Applications	(Thielens, 2013) (Scarfo, 2012)	2
Best Practices	General Best practices Guidelines	(Abubakar Garba et al., 2017) (Romer, 2014) (Alotaibi & Almagwashi, 2018) (Scarfo, 2012) (Hajdarevic et al., 2016) (Fani et al., 2016)	6
Cloud Access	Cloud Computing Cloud Solutions Cloud Storage	(Morrow, 2012) (Scarfo, 2012) (Samaras et al., 2014) (Lennon, 2012) (Downer & Bhattacharya, 2015)	5
Compliance	User compliance Compliance	(Musarurwa et al., 2018) (Ocano et al., 2015)	2
Corporate Data Protection	Data security Data leakage Data exfiltration Data infiltration Data confidentiality Data integrity	(Morrow, 2012) (Garba, Armarego, Murray et al., 2015) (Wang et al., 2014) (Scarfo, 2012) (Petrov & Znati, 2018) (Ocano et al., 2015)	6
Education	Training Awareness Risk awareness Education	(Ketel & Shumate, 2015) (Downer & Bhattacharya, 2015)	2
Governance	C-level Chief Executive Officers Corporate Culture Organizational practice Governance	(Garba, Armarego, Murray et al., 2015) (Baillette et al., 2018) (Ketel & Shumate, 2015) (Fani et al., 2016) (Musarurwa et al., 2018) (Abubakar Garba et al., 2017)	6
IT consumerization	Consumerization	(Vignesh & Asha, 2015) (Scarfo, 2012)	2
Legal	Law Legal issues	(Alotaibi & Almagwashi, 2018)	1
Malware	Computer viruses Malware	(Wang et al., 2014) (Salles-Loustau et al., 2016) (Li et al., 2014) (Chung et al., 2012)	4
Mobile Device Security	Mobile security Electronic devices BYOD solutions Mobile device Deployments Device Security Mobile device mgmt. solutions Device Patches/Upgrades	(Wei et al., 2013) (Wang et al., 2014) (Scarfo, 2012) (Ali et al., 2015) (De las Cuevas et al., 2015) (Downer & Bhattacharya, 2015)	6
Monitoring	Monitoring	(Stoecklin et al., 2016) (Downer & Bhattacharya, 2015)	2
Network	Network Security Mobile Communication Networks Wireless networks Virtual Private Networks Wireless Access Points	(Morrow, 2012) (Zahadat et al., 2015) (Miller et al., 2012) (Musarurwa et al., 2018) (Tokuyoshi, 2013) (Abubakar Garba et al., 2017) (Thielens, 2013) (Wang et al., 2014) (Ketel, 2018) (AlHarthy & Shawkat, 2013)	10

(*Continued*)

Table 2. (Continued).

Security Issues	Keywords (provided in the articles)	Articles	No. of Articles
Policies	Policies	(Cho & Ip, 2018)	11
	Security Policies	(Vignesh & Asha, 2015)	
	Personnel Policies	(Bann et al., 2015)	
	Employment Policies	(Wang et al., 2014)	
	Policy Enforcement	(Salles-Loustau et al., 2016)	
	Policy Implementation	(Ocano et al., 2015)	
		(Ketel & Shumate, 2015)	
		(Hajdarevic et al., 2016)	
		(Downer & Bhattacharya, 2015)	
		(Alotaibi & Almagwashi, 2018)	
		(Armando et al., 2016)	
Risk Management	Enterprise risk management	(Zahadat et al., 2015)	4
	Risk analysis	(Petrov & Znati, 2018)	
	Risk assessment	(Ketel & Shumate, 2015)	
	Risk management	(Hajdarevic et al., 2016)	
Security Management	Security management	(Musarurwa et al., 2018)	2
		(Ketel, 2018)	
Separation of data	Isolation of data	(Wang et al., 2014)	2
	Separation of data	(Ocano et al., 2015)	
User Privacy	Privacy	(Garba, Armarego, Murray et al., 2015)	6
	Data privacy	(Abubakar Garba et al., 2017)	
	Computer privacy	(Salles-Loustau et al., 2016)	
	Employee Privacy	(Alotaibi & Almagwashi, 2018)	
		(Ali et al., 2015)	
		(Miller et al., 2012)	
User Support	Helpdesk	(Scarfo, 2012)	2
		(Hovav & Putri, 2016)	
User/Employee Behavior/Attitude	Employees	(Musarurwa et al., 2018)	8
	Employee behavior	(Abubakar Garba et al., 2017)	
	Employee attitude	(Cho & Ip, 2018)	
	Personal information	(Scarfo, 2012)	
	Intrusiveness	(Lennon, 2012)	
	User compliance	(Giwah, 2018)	
	End-users	(Ocano et al., 2015)	
		(Hovav & Putri, 2016)	
Virtualization	Virtualization	(Petrov & Znati, 2018)	4
		(Ocano et al., 2015)	
		(Ketel, 2018)	
		(Downer & Bhattacharya, 2015)	

devices. There are several variations of these modalities such as choose your own device (CYOD), company owned/personally enabled (COPE), company owned/business only (COBO) and many other flavors of same concept.

Finally, the research criteria of this study can be altered (narrow or broaden) in order to identify more issues, strengthen the existing issues, or focus on different aspects of BYOD.

6. Conclusion

This study presented a systematic review of the literature addressing security issues and considerations related to BYOD phenomena in organizations. Toward this aim we presented a classification scheme based on extant literature. The scheme is comprised of four organizational domains identified as Management, IT, User, and Mobile Device. The objective of the classification scheme is to present a holistic approach when securing BYOD environments, and to provide a basis for identifying and discussing the security issues and responsibilities associated with each domain. It also provides a deeper understanding of the BYOD phenomenon as organizations aim to protect their corporate information.

Using the classification scheme and based on a search criterion, this review identified 38 scholarly articles related to BYOD security. The analysis shows that many security concerns need to be addressed when securing BYOD environments. The review of the selected articles identified 22 issues that have been associated with the organization's domains aforementioned. Based on the analysis performed, it was found that although IT carries the brunt of the security responsibilities, the security of BYOD environments also depends

Table 3. Selected articles. security issues found in each article & classification of articles per domain.

Mg	IT	Usr	Mo Dev	Security Issue	Title and Main Contribution	Reference
x	x	x		Governance, Risk mgmt. User privacy	Title: Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. Analyze the importance of CEO involvement in BYOD security as opposed to the IT initiated approach. This approach discusses the 'reversed IT adoption logic vs the traditional IT adoption logic' in order to balance the induced risks for CEOs and users.	(Baillette et al., 2018)
	x			Network, Corporate data protection, Cloud Access	Title: BYOD security challenges: control and protect your most sensitive data. Discussion of mobile device vulnerabilities. The use of web browsers by customers, 'employees and business partners are accessing information on devices not owned or managed by the organization.'	(Morrow, 2012)
x	x	x		Governance, Network, Risk Management, User Privacy/User behavior	Title: BYOD security engineering: A framework and its analysis Examines risks of allowing BYOD balanced by its benefits. It addresses the security concerns of BYOD, which 'necessitate technology, policy management, and people integration instead of the traditional technology alone approach.' Proposes a BYOD Security Framework as the solution to BYOD security concerns. The framework addresses: People, Policy Management, and Technology as pillars necessary in order to secure BYOD implementations in enterprises.	(Zahadat et al., 2015)
	x	x		User privacy, Network security	Title: BYOD: Security and Privacy Considerations BYOD Security and user privacy concerns are delineated. Discussion of next generation users in terms of BYOD adoption.	(Miller et al., 2012)
x	x	x		Compliance, User behavior, Network, Security Mgmt., Governance	Title: An information security behavioral model for the bring-your-own-device trend The article proposes employee behavioral change for organizations to mitigate the risks that are associated with the BYOD phenomenon. The author discusses six traits for the development of a model that aims to reduce challenges presented by BYOD. The traits include attitude, knowledge, habit, environment, governance and training.	(Musarurwa et al., 2018)
x	x	x		User privacy, Governance	Title: Bring your own device organizational information security and privacy This article reviews information security and privacy, mobile computing, and current organizational practices that shed light on BYOD and the issues behind its adoption. The review assists organizations and IT professionals to understand the increasing demands of BYOD, and its challenges. Discussions include BYOD security controls. Different types of BYOD threats are discussed to include malware, phishing, spoofing, device loss, malicious insiders and policy violation. The research presents three case studies to depict organizational practices.	(Garba, Armarego, Murray et al., 2015)
	x			Network	Title: The security implications of BYOD In addition to discussing the incorporation of new devices into the enterprise outside of the process that IT normally follows for vetting, monitoring and auditing equipment for proper use, this article discusses the importance of securing the network and means to connect to it.	(Tokuyoshi, 2013)
x	x	x		Best practices, User behavior/ attitude, Network, User Privacy, Governance	Title: A systematic approach to investigating how information security and privacy can be achieved in BYOD environments This paper provides best practices approach for BYOD to include security and privacy risks. It focuses on BYOD adoption, and its associated risks and mitigation strategies, investigating how both information security and privacy can be effectively achieved in BYOD. The research presents a case study to understand both organizational and employee views, thoughts, opinions and actions in BYOD environments.	(Abubakar Garba et al., 2017)
	x			Applications, Network	Title: Why APIs are central to a BYOD security strategy The paper discusses the importance of implementation of IT infrastructure that allows employees to use the latest technology, businesses are much more likely to retain, as well as attract, top talent. A secure and scalable BYOD strategy is required to manage the risks introduced by employee-owned devices. The answer may lay in Application Programming Interfaces (APIs). If an organization delivers its data via mobile APIs, then the data does not actually reside on the mobile device.	(Thielens, 2013)
			x	Mobile device security	Title: Corporate Security Solutions for BYOD: A Novel User-Centric and Self-Adaptive System In this paper proposes a taxonomy to classify the features of BYOD systems. This taxonomy is used to present an overview of BYOD security solutions. It also describes a software system named MUSES (Multi-platform Usable Endpoint Security), able to securely manage BYOD environments. MUSES has been developed to cope with security issues with regard to enterprise security policies, but as a user-centric tool.	(De las Cuevas et al., 2015)

(*Continued*)

Table 3. (Continued).

Mg	IT	Usr	Mo Dev	Security Issue	Title and Main Contribution	Reference
x		x		User/employee behavior/ attitude, Policies	Title: A study of BYOD adoption from the lens of threat and coping appraisal of its security policy This study explores the factors affecting employee's adoption intention of BYOD. It presents a theoretical framework that captures the threat from adopting BYOD and coping assessment of security policy for BYOD to include other concerns related to employee's organization commitment and job security.	(Cho & Ip, 2018)
x	x			Policies, IT consumerization	Title: Modifying security policies toward BYOD The article discusses BYOD policies adopted in numerous organizations as vague and generally immature. It proposes a 3-tier enhanced policy architecture which specifies the policies to be followed by the device, applications and organizations.	(Vignesh & Asha, 2015)
	x			Best practices	Title: Best practices for BYOD security This paper discusses the new risks for IT security teams such as security as an afterthought, data contamination, malware, phishing attacks, lost devices, risky file sharing. It proposes best practices that include choosing solutions, centralization, connectivity, cloud control, and blocking of risky services.	(Romer, 2014)
	x	x		End-user behavior, User support/helpdesk	Title: This is my device! Why should I follow your rules? Employees' compliance with BYOD security This article examines the factors that determine employees' intention to comply with BYOD policies. The results show that IT support and balance of mutual benefit positively affect compliance, where the threat of reduced freedom negatively affect policy compliance.	(Hovav & Putri, 2016)
x	x			Access control, Policies	Title: Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment This paper discusses BYOD vulnerabilities resulting from APT via spear phishing attacks and the mediation of that type of attack through the implementation of security policies. The authors propose the implementation of access control policies consistent with MAC (mandatory access control) as the best way to mitigate spear phishing attacks.	(Bann et al., 2015)
	x			Access control	Title: Facial Biohashing Based User-Device Physical Unclonable Function for Bring Your Own Device Security This paper discusses authentication schemes to ensure the authorized user has access to the device. It proposes an algorithm (a biohashing technique) to authenticate both the user and the device.	(Zheng et al., 2018)
	x		x	Mobile device	Title: T-dominance: Prioritized Defense Deployment for BYOD Security This article introduces an algorithm that groups the mobile devices based on their behavior thus prioritizing the security stringiness on the device. Instead of employing the same costly and intrusive security measures on each BYOD smartphone, more stringent threat detection/mitigation mechanisms are deployed on those representative smartphones, each of which represents, security-wise, a group of smartphones in the whole BYOD device pool.	(Wei et al., 2013)
x	x		x	Corporate data protection, Mobile device, Separation of data	Title: Bring Your Own Device Security Issues and Challenges This article presents threats and attacks on BYODs and discusses security issues. The paper further compares existing BYOD solutions and presents a BYOD security framework that provides guidance for enterprises when adopting BYODs.	(Wang et al., 2014)
	x			Monitoring	Title: Passive security intelligence to analyze the security risks of mobile/BYOD activities This paper introduces an algorithm that passively monitors BYOD usage without the need to install an agent. It provides information such as device type, model, OS, applications and patch levels.	(Stoecklin et al., 2016)
x	x	x	x	Cloud access, Applications, Best practices, Corporate data protection, User/employee behavior/ attitude, IT consumerization, Mobile device, User support	Title: New security perspectives around BYOD This informative paper presents a survey with respect to BYOD trend, concerns and modalities for access control and device control, all from a security perspective.	(Scarfo, 2012)
	x			Cloud access	Title: An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD This paper describes the different dimensions of information security architecture to secure SaaS applications that are accessed via BYOD. It proposes a framework for enterprises that access SaaS cloud services by Smartphone BYOD. This architecture is based on the SABSA security architecture framework, which consists of the hardware, software and service-oriented security components that can reduce the aforementioned risks to acceptable levels	(Samaras et al., 2014)

(*Continued*)

Table 3. (Continued).

Mg	IT	Usr	Mo Dev	Security Issue	Title and Main Contribution	Reference
	x	x		Malware, Policies, User Privacy	Title: Don't just BYOD, Bring-Your-Own-App Too! Protection via Virtual Micro Security Perimeters The authors propose a system (SWIRLS) to protect data and data owners rather than apps and services within the BYOD. The system allows security and privacy policies to be attached to individual pieces of data in order to provide data protection and data isolation.	(Salles-Loustau et al., 2016)
	x			Access control, Corporate data protection, Risk management, Virtualization	Title: Context-Aware Deep Learning-Driven Framework for Mitigation of Security Risks in BYOD-Enabled Environments This paper discusses existing techniques to protect against BYOD risks, to include MDM and virtualization. It proposes a framework for identifying non-legitimate users who try to get access to organization's critical infrastructure.	(Petrov & Znati, 2018)
x	x	x	x	Compliance, Corporate data protection, User/employee behavior, Policies, Separation of data, Virtualization	Title: Remote Mobile Screen (RMS): an approach for secure BYOD environments This paper discusses a plethora of security issues related to BYOD. These include space isolation, data confidentiality and policy compliance as well as handling the resource constraints of the device and issues related to intrusiveness. It proposes an approach (RMS) to secure BYOD environments that addresses the aforementioned issues.	(Ocano et al., 2015)
x		x		Network, User privacy	Title: BYOD: Security and Privacy Considerations The authors discuss BYOD security concerns with respect to network connectivity and privacy concerns. The paper also discusses next-generation users.	(Miller et al., 2012)
	x			Malware	Title: Feedback-based smartphone strategic sampling for BYOD security This article discusses security issues related to malware in BYOD as a major security concern. The authors propose a method that improves BYOD security mechanisms to improve malware detection.	(Li et al., 2014)
		x		Cloud access, User/Employee Behavior/ Attitude	Title: Changing User Attitudes to Security in Bring Your Own Device (BOYD) & the Cloud The paper discusses the security risks related to cloud environments. Special attention is given to BYOD users accessing cloud resources and their attitude toward the reevaluation of the security of their own devices.	(Lennon, 2012)
x	x	x		Education, Policies, Risk Management, Governance	Title: Bring Your Own Device: Security technologies This paper discusses mitigation of BYOD risks which include policies, technologies, education and training.	(Ketel & Shumate, 2015)
	x			Network, Virtualization, Security mgmt.	Title: Enhancing BYOD Security through SDN This paper discusses technological solutions that organizations can implement to secure BYOD environments. Emphasis is made on network technologies such as Software Define Networking (SDN) and Network Functions Virtualization (NFV). Other solutions are essential for organizations to manage and secure BYOD to include technologies for managing mobile devices (MDM), application (MAM), and content (MCM).	(Ketel, 2018)
x	x			Policies, Risk mgmt., Best practices	Title: Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments This paper discusses best practices and standards for BYOD security as it relates to the ISO 27000 standards. It proposes an approach to creating metrics which can be used to align security policies with BYOD policy.	(Hajdarevic et al., 2016)
x		x		User behavior	Title: User Information Security Behavior Toward Data Breach in Bring Your Own Device (BYOD) Enabled Organizations – Leveraging Protection Motivation Theory. This paper discusses security concerns related to the behavioral intent of BYOD employees (i.e. negligence or noncompliance) when carrying organizational data in their mobile devices and thus exposing the organization to security breaches. The paper proposes a conceptual model based on Protection Motivation Theory (PMT).	(Giwah, 2018)
x				Governance, Best practices	Title: Governing information security within the Context of "Bring Your Own Device in SMMEs" This paper provides 'basic guideline to Executive Management on how they can govern and manage the BYOD phenomenon in Small-Medium Micro Enterprises' (SMMEs). The authors discuss how these businesses are affected, list risk factors and provide guidelines for best practices and information security.	(Fani et al., 2016)
x	x	x	x	Cloud access, Education, Monitoring, Policies, Mobile device, Virtualization	Title: BYOD Security: A New Business Challenge This paper addresses BYOD security challenges that touch all domains of an organization. It also discusses available frameworks. It presents a classification scheme which includes challenges for deployment, technical, policy, and human aspects.	(Downer & Bhattacharya, 2015)

(*Continued*)

Table 3. (Continued).

Mg	IT	Usr	Mo Dev	Security Issue	Title and Main Contribution	Reference
	x			Access control, Malware	Title: 2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security This paper discusses security issues related to access control and malware among others. The authors present an architecture called 2-Tier Access Control (2TAC) which uses 'double layer access control along with device security profiles, ant-virus/malware scanners and social networking.	(Chung et al., 2012)
	x			Policies	Title: Developing a NATO BYOD Security Policy With respect to policies, this paper presents a proposal of 'how to foster a secure, policy-aware BYOD work environment.' After consulting with NCI Agency and extracting security rules from existing guidelines suitable for BYOD, the proposed security framework (BYODroid) involves 'enforcement of fine-grained security policies for personal devices while relieving owners of having to make critical decisions and take responsibility for behavior of applications installed on their devices.' The results involve modeling and enforcing actual security policies for a complex BYOD environment such as NCI Agency.	(Armando et al., 2016)
x	x			Best practices, Legal, Policies, User privacy	Title: A Review of BOYD Security Challenges, Solutions and Policy Best Practices The paper review BYOD security and privacy issues, management approaches to include network solutions, mobile device management approaches, and policy best practices from an organizational point of view. It presents a BYOD security-policy architecture based on best practices for information security and privacy controls in three levels: device level, application level and organizations level.	(Alotaibi & Almagwashi, 2018)
x	x	x	x	Access control, Mobile device, User privacy	Title: Analysis of BYOD Security Frameworks This paper 'analyzes threats associated with BYOD, presents security requirements and provides classification of BYOD security models as discussed in the literature till date.' The authors propose a model that meet all the stated security requirements for BYOD.	(Ali et al., 2015)
	x			Network	Title: Implement network security control solutions in BYOD environment The authors discuss network security issues related to BYOD where the research describes network security solution implemented in Oman. The paper focuses on a set of principles that need to be followed where emphasis is made on network security for IT to follow.	(AlHarthy & Shawkat, 2013)
Tot 19	32	17	7			

on management decisions, the BYOD users, and the security of the mobile device itself. The analysis of the security issues shows that concerns related to the implementation of policies is the number one security issue related to BYOD. This is followed by issues associated with the network, protection of the corporate data, user's behavior, and governance.

Reflecting on the findings, we conclude that a holistic approach to security is needed in order

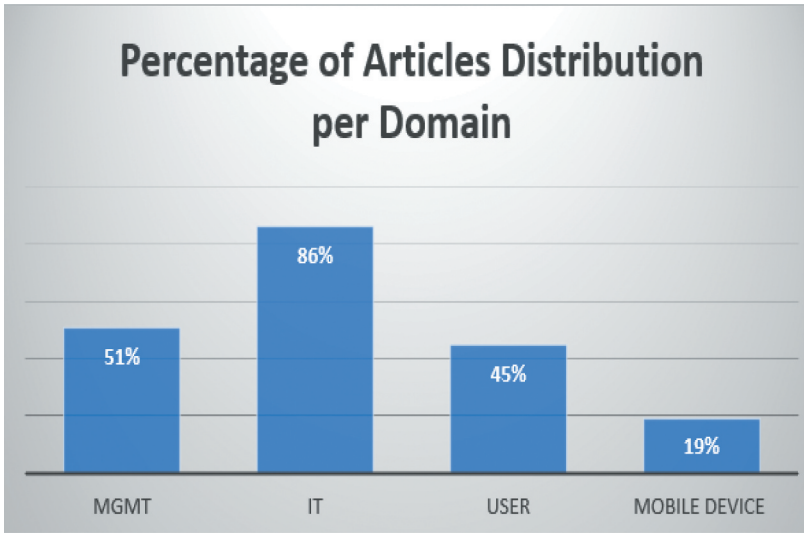

Figure 6. Percentage of published articles distribution per domain.

Table 4. Concentration of articles based on security issues.

Security Issues & Considerations	No. of Articles
Policies	12
Network	10
Corporate Data Protection	8
User/Employee Behavior/Attitude	8
Governance	7
Best Practices	6
Mobile Device Security	6
User Privacy	6
Access Control	5
Cloud Access	5
Malware	4
Risk Mgmt.	4
Virtualization	4
Applications	2
Compliance	2
Education	2
IT consumerization	2
Monitoring	2
Security Management	2
Separation of data	2
User Support/Helpdesk	2
Legal	1

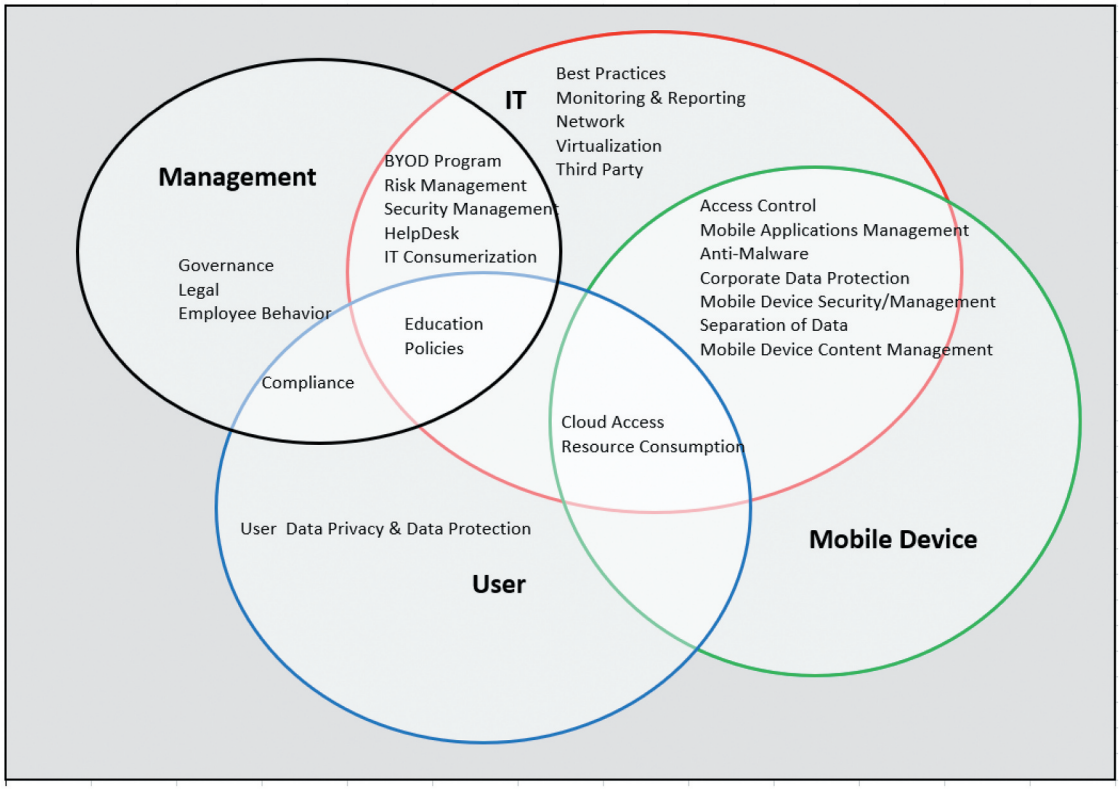

Figure 7. Overlap of security issues across domains.

to implement security countermeasures associated with all four domains of any organization. Future research can address the need and importance of systematically addressing all four domains to ensure a comprehensive approach to BYOD security. Moreover, a holistic approach to BYOD security implies a better understanding of the extent of overlap of various security issues across these organizational domains. Other areas for consideration include further exploration of issues with low article concentration and the identification of relevant controls associated with the security issues.

Overall, the BYOD phenomenon is fertile ground for research that aims to protect

organizations that adopt BYOD. This systematic literature review has implications to theory and practice. With respect to the former, this review helps to understand the BYOD phenomenon. The classification scheme and definitions provide bases for expansion of security concepts related to BYOD and the continued exploration of holistic approach to security. From the practical point of view, the information presented in this study informs the organization's decision makers of the risks when adopting BYOD, and aids practitioners when discussing the adoption of security safeguards. It also stresses the importance of adopting a holistic/comprehensive approach to security as the organization's upper management makes decisions that affect the security of the corporation and its information.

References

27001Academy. (2017a). *Clause-by-clause explanation of ISO 27001*.

27001Academy. (2017b). *Diagram of ISO 27001 risk assessment and treatment process*. https://cdn2.hubspot.net/hubfs/1983423/27001Academy/27001Academy_FreeDownloads/Diagram_of_ISO_27001_risk_assessment_and_treatment_process_EN.pdf?utm_campaign=free-resources-27001&utm_source=hs_automation&utm_medium=email&utm_content=50020281&_hsenc=p2ANqtz-9usCc12nPeBCl58pNYflh5gx18Bg9LW8KEbJ1DA14CtobtaTzfDCg1LZTt8iwF2p89dad7iJSIqK4J7gNi4JzA_SWxvYVFUwAM1wolyYaoaIRt-gE&_hsmi=50020281

Absalom, R. (2012). International data privacy legislation review: A guide for BYOD policies. *Ovum Consulting, IT006*, *234*, 3–5.

Abubakar Garba, B., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security*, *25*(4), 475–492. doi:http://dx.doi.org/10.1108/ICS-03-2016-0025

AlHarthy, K., & Shawkat, W. (2013, 29 Nov.-1 Dec. 2013). *Implement network security control solutions in BYOD environment. Paper presented at the 2013 IEEE International Conference on Control System, Computing and Engineering.*

Ali, S., Qureshi, M. N., & Abbasi, A. G. (2015, 18–18 Dec. 2015). *Analysis of BYOD security frameworks. Paper presented at the 2015 Conference on Information Assurance and Cyber Security (CIACS).*

Alotaibi, B., & Almagwashi, H. (2018, 4–6 April 2018). A review of BYOD security challenges, solutions and policy best practices. Paper presented at the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). IEEE

Amoud, M., & Roudies, O. (2017). *Experiences in secure integration of Byod. Paper presented at the Proceedings of the 7th International Conference on Information Communication and Management*, Moscow, Russian Federation.

Armando, A., Costa, G., Merlo, A., Verderame, L., & Wrona, K. (2016, 23–24 May 2016). Developing a NATO BYOD security policy. Paper presented at the 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEE

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004b). Basic concepts and taxonomy of dependable and secure computing. IEEE Consumer Electronics Magazine, 1, 1. IEEE transactions on dependable and secure computing

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management*, *43*, 76–84. https://doi.org/doi:10.1016/j.ijinfomgt.2018.07.007

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted security policies for tackling advanced persistent threat via Spear Phishing in BYOD environment. *Procedia Computer Science*, *72*, 129–136. https://doi.org/doi:10.1016/j.procs.2015.12.113

Bello Garba, A., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, *10*(3), 1279–1287.

CCMB- 2012-09-001. (2012). *Common criteria for information technology*.

Cho, V., & Ip, W. H. (2018). A study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems*, *12*(6), 659–673. https://doi.org/doi:10.1080/17517575.2017.1404132

Chung, S., Chung, S., Escrig, T., Bai, Y., & Endicott-Popovsky, B. (2012, 14–16 Dec. 2012). *2TAC: Distributed access control architecture for "Bring Your Own Device" security. Paper presented at the 2012 ASE/IEEE International Conference on BioMedical Computing (BioMedCom).*

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with Bring Your Own Device policies utilizing protection motivation theory: bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226. https://doi.org/doi:10.2308/isys-50704

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., García-Sánchez, P., & Fernández-Ares, A., & de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., García-Sánchez, P., & Fernández-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, *68*, 83–95. https://doi.org/doi:10.1016/j.comcom.2015.07.019

Disterer, G. (2013a). *Iso/iec 27000, 27001 and 27002 for information security management*. http://file.scirp.org/Html/4-7800154_30059.htm

Disterer, G. (2013b). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 9. https://doi.org/doi:10.4236/jis.2013.42011

Downer, K., & Bhattacharya, M. (2015, 19–21 Dec. 2015). *BYOD security: A new business challenge. Paper presented at the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*.

Fani, N., Solms, R. V., & Gerber, M. (2016, 11–13 May 2016). Governing information security within the context of "bring your own device in SMMEs". *Paper presented at the 2016 IST-Africa Week Conference*.

Garba, A. B., Armarego, J., & Murray, D. (2015). A policy-based framework for managing information security and privacy risks in BYOD environments. *International Journal of Emerging Trends & Technology in Computer Science*, *4*(2), 189–198.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information Privacy & Security*, *11*(1), 38–54. http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/1691289631?accountid=27073 .

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gimenez, S., Ramamurthy, B., & Wang, Y. (2015). *A survey on extending the organization's network using the Bring Your Own Device (BYOD) environment*. Technical Report, University of Nebraska-Lincoln.

Giwah, A. D. (2018, 19-22 April 2018). *User information security behavior towards data breach in Bring Your Own Device (BYOD) enabled organizations - leveraging protection motivation theory. Paper presented at the SoutheastCon 2018*.

Grundshutz. (2004). *Grundshutz IT manual elementary threats*.

Grundshutz, G. I. *German IT Grundshutz Suplement overview excerpts*

Guttman, B., & Roback, E. A. (1995). *Sp 800-12*. the NIST handbook.

Hajdarevic, K., Allen, P., & Spremic, M. (2016, 22–23 Nov. 2016). *Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments. Paper presented at the 2016 24th Telecommunications Forum (TELFOR)*.

Hernandez, A., & Choi, Y. (2014). Securing BYOD networks: Inherent vulnerabilities and emerging feasible technologies. *International Journal of Computer and Information Technology*, *3*(5).

Herrera, A. V., Ron, M., & Rabadão, C. (2017). *National cyber-security policies oriented to BYOD (bring your own device): Systematic review. Paper presented at the Information Systems and Technologies (CISTI), 2017 12th Iberian Conference on*.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49. https://doi.org/doi:10.1016/j.pmcj.2016.06.007

ISACA. (2016). *IS Audit/Assurance program for BYOD*. www.isaca.org

ISACA. (2019a). *ISACA cybersecurity fundamentals glossary*. https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

ISACA. (2019b). *ISACA glossary*. https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Ketel, M. (2018, 19-22 April 2018). *Enhancing BYOD security through SDN. Paper presented at the SoutheastCon 2018*.

Ketel, M., & Shumate, T. (2015, 9–12 April 2015). *Bring Your Own Device: Security technologies. Paper presented at the SoutheastCon 2015*.

Kiely, L., & Benzel, T. V. (2006). Systemic security management. *IEEE Security & Privacy*, *4*(6), 74–77. https://doi.org/10.1109/MSP.2006.167

Lennon, R. G. (2012, 25–27 Oct. 2012). *Changing user attitudes to security in bring your own device (BYOD) & the cloud. Paper presented at the 2012 5th Romania Tier 2 Federation Grid, Cloud & High Performance Computing Science (RQLCG)*.

Li, F., Huang, C., Huang, J., & Peng, W. (2014, 4–7 Aug. 2014). *Feedback-based smartphone strategic sampling for BYOD security. Paper presented at the 2014 23rd International Conference on Computer Communication and Networks (ICCCN)*.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *PLoS Medicine*, *6*(7), e1000100. https://doi.org/10.1371/journal.pmed.1000100

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*. CRC Press.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, *14*(5), 53–55. https://doi.org/doi:10.1109/MITP.2012.93

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. doi:http://dx.doi.org/10.1016/S1353-4858(12)70111-3

Moyer, J. E. (2013). Managing mobile devices in hospitals: A literature review of BYOD policies and usage. *Journal of Hospital Librarianship*, *13*(3), 197–208. https://doi.org/10.1080/15323269.2013.798768

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *South African Journal of Information Management*, *20*(1). doi:http://dx.doi.org/10.4102/sajim.v20i1.980

Ngai, E. W., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Ocano, S. G., Ramamurthy, B., & Wang, Y. (2015, 16–19 Feb. 2015). *Remote mobile screen (RMS): An approach for secure BYOD environments. Paper presented at the 2015 International Conference on Computing, Networking and Communications (ICNC).*

Ogie, R. (2016). Bring Your Own Device: An overview of risk assessment. *IEEE Consumer Electronics Magazine*, *5*(1), 114–119. https://doi.org/doi:10.1109/MCE.2015.2484858

Oktavia, T., Yanti, H., Prabowo, H., & Meyliana, H. (2016). *Security and privacy challenge in Bring Your Own Device environment: A systematic literature review*. In (pp. 194–199).

Petrov, D., & Znati, T. (2018, 18–20 Oct. 2018). *Context-aware deep learning-driven framework for mitigation of security risks in BYOD-enabled environments. Paper presented at the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).*

Ratchford, M. M., & Wang, Y. (2019). *BYOD-insure: A security assessment model for enterprise BYOD. Paper presented at the 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ).*

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security*, *2014*(1), 13–15. https://doi.org/doi:10.1016/S1361-3723(14)70007-7

Salles-Loustau, G., Garcia, L., Joshi, K., & Zonouz, S. (2016, 28 June-1 July 2016). *Don't just BYOD, Bring-Your-Own-App Too! Protection via virtual micro security perimeters. Paper presented at the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).*

Samaras, V., Daskapan, S., Ahmad, R., & Ray, S. K. (2014, 26–28 Nov. 2014). *An enterprise security architecture for accessing SaaS cloud services with BYOD. Paper presented at the 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC).*

Scarfo, A. (2012, 12–14 Nov. 2012). *New security perspectives around BYOD. Paper presented at the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.*

Scarfone, K. A., Souppaya, M. P., & Hoffman, P. (2011). *Sp 800–125. guide to security for full virtualization technologies.*

Shirey, R. W. (2000). *Internet security glossary.*

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Souppaya, M., & Scarfone, K. (2013). NIST special publication 800-124 guidelines for managing the security of mobile devices in the enterprise. *Gaithersburg, USA: National Institute of Standards and Technology*, (1–29).

Souppaya, M., & Scarfone, K. (2016a). *NIST 800–46 rev 2 guide to enterprise telework, remote access, and Bring Your Own Device (BYOD) security*. http://csrc.nist.gov/publications/drafts/800-46r2/sp800_46r2_draft.pdf

Souppaya, M., & Scarfone, K. (2016b). *NIST 800–114 rev 1 user's guide to telework and Bring Your Own Device (BYOD) security*. http://csrc.nist.gov/publications/drafts/800-114r1/sp800_114r1_draft.pdf

Stoecklin, M. P., Singh, K., Koved, L., Hu, X., Chari, S. N., Rao, J. R., Cheng, P.-C., Christodorescu, M., Sailer, R., & Schales, D. L. (2016). Passive security intelligence to analyze the security risks of mobile/BYOD activities. *IBM Journal of Research and Development*, *60*(4), 9:1–9:13. https://doi.org/doi:10.1147/JRD.2016.2569858

Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security*, *2013*(8), 5–6. doi:http://dx.doi.org/10.1016/S1353-4858(13)70091-6

Thompson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2). http://dx.doi.org/10.1016/S1353-4858(12)70013-2 .

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, *2013*(4), 12–13. http://www.sciencedirect.com/science/article/pii/S1353485813700503

United-Kingdom. (2012). *Businesses failing to communicate bring your own device best practice to employees. MENA Report*, *http://www.ezproxy.dsu.edu:2048/login?url=https://www.ezproxy.dsu.edu:2206/docview/1080987877?accountid=27073*

Utter, C., & Rea, A. (2015). The 'Bring Your Own Device' Conundrum form Organizations and Investigators: An Examination of the Policy and Legan Concerns in Light of Investigatory Challenges. *Journal of Digital Forensics, Security & Law, V*, *10*(2), 55.

Vignesh, U., & Asha, S. (2015). Modifying Security Policies Towards BYOD. *Procedia Computer Science*, *50*, 511–516. https://doi.org/doi:10.1016/j.procs.2015.04.023

Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Wang, Y., Wei, J., & Vangury, K. (2014). *Bring your own device security issues and challenges. Paper presented at the Consumer Communications and Networking Conference (CCNC)*, 2014 IEEE 11th.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii–xxiii.

Wei, P., Feng, L., Han, K. J., Xukai, Z., & Jie, W. (2013, 14–16 Oct. 2013). *T-dominance: Prioritized defense deployment for BYOD security. Paper presented at the 2013 IEEE Conference on Communications and Network Security (CNS)*.

Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013, 8–14 Sept. 2013). *Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior. Paper presented at the 2013 International Conference on Social Computing.*

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99. https://doi.org/10.1016/j.cose.2015.06.011

Zheng, Y., Cao, Y., & Chang, C. (2018, 12–14 Jan. 2018). *Facial biohashing based user-device physical unclonable function for bring your own device security. Paper presented at the 2018 IEEE International Conference on Consumer Electronics (ICCE).*