Emergent BYOD Security Challenges and Mitigation Strategy

Authors: Ahmed Dedeche, Fenglin Liu, Michelle Le, Saeed Lajami

Abstract

There is limited research and literature on the topic of 'Bring-your-own-device' (BYOD) in organizations. BYOD is a new business trend where employees are using their own devices for work purposes. This phenomenon has introduced new security challenges to the business environment. Traditionally, organizational security risks have been addressed by adapting various established Information Security (IS) strategies. This research paper aims to identify how these strategies can be implemented by organizations to address the emergent BYOD risks.

Introduction

Many organizations are increasingly turning to Information Technology as a means for productivity gains and reduction of operating costs. A study by the Society of Information Management (SIM) in 2011 showed that 'business productivity and cost reduction' is a key priority for global organizations, ranking fourth on the list of top management concerns for that year. A number of emergent technologies were also identified, with 'mobile and wireless technologies' the fastest growing area for technology investment globally (Lufman et al. 2012). The rapid adoption of smartphones and tablets has led to the 'Consumerization of IT' or diffusion of consumer devices into the enterprise (Thomson, 2012). To meet the mobility demands of today's employees, organizations have started to embrace BYOD to realize productivity gains and cost benefits from allowing employees to use their technology of choice in the workplace. While new technologies have the potential to bring significant legitimate business benefits, they are also vulnerable to criminal exploitations; giving rise to new forms of Information Security (IS) risks (Grabosky, 2007).

This paper explores the emerging phenomenon of BYOD and the associated IS challenges, and discusses how established IS strategies, such as 'Defense-in-depth', can be applied to mitigate identified emergent risks such as data leakage. It is divided into three sections. Section 1 introduces the concept of BYOD and describes the research methodology taken. Section 2 presents a literature review of established IS strategies, the current BYOD landscape, and the most frequently identified IS risks and challenges. Section 3 discusses current approaches used by organizations to mitigate these risks and what can be done, from an IS strategy perspective, to improve the resilience of an organization's BYOD information security.

This paper will contribute to IS personnel's understanding and awareness of BYOD and the associated security challenges, and lead them to review implemented BYOD strategies in their organization, as well as inform the creation of new strategies.

Research Methodology

We developed our Information Security (IS) strategy perspective on BYOD security by conducting a literature review on publications from high quality journals. We used the EBSCO, Science Direct, Google Scholar, and ProQuest databases to search for literature using the following keywords: information security strategy, BYOD, bring your own device, security and mobility, MDM, Mobile

Device Management, managing BYOD, BYOD security, and IT consumerization. We divided the literature review into two distinct sections: IS Strategy and BYOD.

For IS Strategy, we selected the peer-reviewed paper "Information security strategies: towards an organizational multi-strategy perspective" by Ahmad et al. (2012) as the primary literature for review. Firstly, this paper provides clear theoretical and practical explanations for established IS strategies. Eleven security experts were involved in the research to provide input from practical experience. Secondly, this paper draws upon rich knowledge and academic evidence of IS strategy, with a total of 121 references to publications from 1975 to 2012. Thirdly, this paper proposed interesting findings and deep discussions on the implementation of identified IS strategies within organizations. Thus, the paper provided a sound theoretical foundation for the analysis of IS issues in BYOD from a strategic perspective.

For BYOD, the primary literature reviewed is "BYOD: enabling the chaos" by security industry expert Gordon Thomson. Firstly, this paper has been published in a reputable academic journal in Elsevier's Network Security journal. Secondly, the paper presented deep analysis of both technical and non-technical aspects of BYOD from a practical experience. As BYOD is a relatively new phenomenon, limited literature exists on the associated IS challenges and the current approaches adopted by organizations. However, these security risks have been discussed in recent journal articles, conference papers and professional literature. A large number of additional publications were also reviewed to build the authors' knowledge of BYOD and the associated risks to arrive at the conclusion.

Literature Review

Information Security Strategy

Some strategists define organizational strategy as the "utilization of limited organizational resources to compete in the business world" through the "creation of a unique and valuable position, involving a different set of activities" (Porter, 1996; Wang, 2005). Furthermore, IS strategy is defined as the establishment of "a security positioning that fits with the company's resources and business direction" in order to defend the "organization's information infrastructure(s) against internal and external threats" (Wang, 2005; Park and Ruighaver, 2008). IS strategy will aid in the creation and implementation of organizational security policies (Straub et al. 2008), with current literature identifying the primary IS strategies to be Prevention,

Deterrence, Surveillance, Detection, Response, Perimeter Defense, Compartmentalization and Layering (Ahmad et al. 2012).

The Need for IS strategy

The speed of organizational technological change has been accelerating in recent years. While new technologies are important drivers for innovation and is critical for competitive advantage, it also introduces a range of security challenges. A survey by leading consulting firm, Ernst & Young (2012), found that "Emerging technologies risk was identified as number 5 in a list of top 10 risks to be faced by businesses in the coming years". Without appropriate IS strategic planning and investment, security enhancements will continue to lag behind the rise in threats. The same survey identified that "the gap between necessary IS levels and actual IS levels continues to grow" (Ernst & Young, 2012). Thus, new technology introduced into the organizational network must be governed by appropriate IS measures to ensure this gap does not widen further. Some researchers suggest that this can be achieved by building an IS strategy that encompasses a "comprehensive framework to enable the development, institutionalization, assessment, and improvement of an information security program." (Ahmad et al. 2012)

Established IS strategies

Prevention

Prevention is the most common security strategy implemented by organizations to proactively protect information assets from being attacked or exploited (Ahmad et al. 2012; Liu et al., 2001). For example, a firewall is often used to protect computer networks against potentially malicious external threats. However, a preventive mindset may encourage organizations to focus on absolute protection at the expense of usability of the asset (Ahmad et al. 2012). Prevention strategies also have a time and space limitation. It is known that "It's too late to sharpen your sword when the drum beats for battle", however in reality, most organizations only pay attention to an IS risk after the incident has occurred (Sveen et al. 2009). This is perhaps attributed to limited organizational resources and the significant costs associated with absolute defense (Anderson, 2001).

Detection

Detection aims to identify specific security behavior including malicious or unusual behavior, intrusion, misuse, and specific attacks against information assets (Ahmad et al. 2012). Due to the challenges of absolute prevention, this strategy is gaining popularity with fast adoption of intrusion detection systems (IDS) as organizations realize the potential value gained from having a

properly configured IDS system within its overall IS strategy (Cavusoglu et al. 2005). For example, IDS allows organizations to continuously scan their computer network devices and detect security anomalies.

Organizations must also consider how to efficiently gain insights from the information collected by IDS systems to inform IS strategies, ensure effective security responses, and support managerial decision-making. According to Ahmad et al. (2012), this information should be "actionable and useful" with relevant information such as the time and scope of attack.

Response

Once an attack has been detected and identified, a response strategy will guide the organization in executing appropriate security countermeasures (Ahmad et al. 2012). Therefore, detection and response are complementary strategies that work together to effectively protect against attacks. As Scheiner (2003) states, "Detection is useless without response." Response strategies primarily focus on reaction and recovery. The former refers to the combined defensive and offensive actions (Tirenin & Faatz, 1999), while the latter refers to the restoration of information assets to a normal state. For example, a response to the detection of a computer virus may involve blocking the compromised port, and in extreme cases isolation, to prevent propagation of the virus across the company network (Ahmad et al. 2012). Thus, a response strategy is necessary to minimise the impact of an incident and to prevent reoccurrence.

Compartmentalization

Compartmentalization is a strategy that aims to contain the damage of attacks by dividing information assets or infrastructures into segregated protected zones. For example, technologies such as classified data servers have the ability to partition information assets. If an intruder defeats the security of one zone they will not be able to wreak havoc on another, thus providing more time for organizational IS teams to take corrective actions before other zones are compromised (Tirenin & Faatz, 1999). This strategy has proven useful for the control of corporate mobile devices. A survey by Ahmad et al. (2012) found that some firms only allowed unauthorized mobile devices to connect to isolated network zones that have been separated from its internal network.

However, there are major issues with a compartmentalization strategy. Firstly, organizations must sacrifice the information assets under attack in one zone to save the whole 'ship' (Tirenin & Faatz, 1999). Secondly, security factors such as sensitivity of data, user privilege and proxy configurations must be predefined prior to developing segregated zones. Thirdly, how long will an isolated zone survive and at what cost? Therefore, many factors must be considered when

developing and implementing a compartmentalization strategy. Tirenin and Faatz (1999) purport that system and network interdependencies must be known prior to strategy implementation, which can make it complex.

Isolation (deception)

Isolation aims to lure and trap the intruder inside a controlled zone inside an organization's computer network to monitor and analyze their actions (Tirenin & Faatz, 1999). This can also be referred to as a Deception strategy where decoys are used to divert an intruder's time and resources from attacking critical information assets (Ahmad et al. 2012). This strategy allows IS teams to monitor and analyze the behavior of malicious intruders. This information can be fed into an organization's IDS to improve detection of suspicious behaviors in future. Some authors believe that isolation allows organizations to gather critical information on attackers that can be used to enhance their security readiness in preventing, detecting and responding to unknown risks in future (Tirenin & Faatz, 1999).

Deterrence

Deterrence aims to influence human behavior and attitude through utilization of disciplinary measures or policies to deter people from engaging in insecurity activities (Ahmad et al. 2012; Hu et al. 2011). A key component of this strategy is an organizational culture that promotes security. Hence, in addition to developing security policies and penalties for non-compliance, organizations must also consider non-technical aspects such as education and training, security awareness, computer abuse, moral standards and self-control (Ahmad et al. 2012; Hu et al.2011; Park et al. 2011).

However, this strategy is not widely employed by organizations for a number of reasons. Firstly, the non-technical concepts of a deterrence strategy may be difficult for IS personnel to grasp as many view security through a technical lens (Sveen et al. 2009). Secondly, albeit having long-term effects, it also requires a longer time to implement (Sveen et al. 2009). Thirdly, this strategy is dependent on employees' level of self-control and moral beliefs and is thus more susceptible to failure (Hu et al. 2011). Ahmad et al.'s (2012) survey found that strict deterrence regimes could be unsuccessful in influencing desired behavior as employees often find new ways to circumvent security controls.

Surveillance

Surveillance aims to monitor the organizational security environment and maintain high situational awareness thus allowing the organization to quickly adapt to emerging security risks and threats. According to Ahmad et al. (2012), it is a challenging task to holistically monitor

technical and non-technical aspects of an organization's IS environment, both in the terrestrial and digital world. Firstly, this is attributed to the complexity of the security environment, which makes it difficult to determine the appropriate location for monitoring 'sensors'. Secondly, efficient management including backup, storage, analysis and deletion of the high volumes of data captured via monitoring logs can be time and resource intensive.

Layering (Defense-In-Depth)

Offense is easier than defense due to the inherent information asymmetry between the two (Tierenin and Faatz, 1999; Anderson, 2001). An attacker with limited resources is able to successfully break through any security defense by focusing on exploitation of a single unknown vulnerability or creating a new vulnerability. On the other hand, absolute defense requires significant resources and knowledge (Anderson, 2001). Layering, or 'Defense-in-Depth', is the implementation of varied and independent defense technologies to increase the perceived costs of attacks (time and expertise), thus deterring potential offenders. The layering of simpler security measures is a cost effective strategy for countering the problem of information asymmetry between offense and defense (Ahmad et al., 2012; Tierenin and Faatz, 1999; Anderson, 2001). Several studies have shown defense-in-depth to be an effective strategy for protecting information assets as vulnerabilities in one technology can be mitigated by strengths in another (Tirenin and Faatz, 1999; Ahmad et al. 2012). It is important to utilize varied defense mechanisms that do not share common-node vulnerabilities that can be easily compromised (Tirenin and Faatz, 1999).

The defense-in-depth strategy can also extend to implementation of non-technical layers such as security policy and processes, training and awareness and culture.

Bring Your Own Device (BYOD)

What is BYOD?

BYOD describes the emergent business trend of using employee-owned technologies in the workplace. It is part of the broader phenomenon of "IT consumerization", which refers to the dual use of employee personal devices and software for private and professional purposes within enterprises (Moschella et al. 2004, cited in Niehaves et al. 2013). Some authors purport that BYOD represents a paradigm shift in the utilisation and management of terminal devices in the workplace (Armando et al. 2013). By definition, "an employee's personal device is one that has not been configured and locked down by the organisational IT department" (Mansfield-Devine, 2012), and thus is vulnerable. BYOD also allows organizations, the conventional providers of workplace

IT, within the workplace, are now transferring the liability of provisioning and maintaining the device to their employees (Mobile Enterprise, 2011, cited in Caldwell et al. 2012). Thomson (2012) indicates that organisations are strategically moving from a "managed world to an unmanaged or 'borderless' world", where there is an undefined security perimeter and IT no longer manages every organisational information asset. A 2011 study by Mobile Enterprise, cited in Caldwell et al. (2012), found that corporations are liable for only 35% of smartphones in the workplace, suggesting that 63.5% are personal devices that have access to company resources.

How Did BYOD Emerge?

The BYOD trend has a number of underlying business drivers. Firstly, organisations are responding to a generational shift in expectations from their employees who demand job flexibility and desire to perform their work on the latest technological gadgets (Gatewood, 2012; Thomson, 2012). Some authors argue that employees today have an expectation of being "able to access whatever they need from wherever in order to their jobs", and are more productive using self-selected technologies that are not "officious, obstructive, or even…old-fashioned" (Mansfield-Devine, 2012; Thomson, 2012). Thus BYOD is a response to growing pressure from the connected workforce of tomorrow and is a tactic for attracting and retaining top talent.

Paul French, Vice President of Product and Solutions Marketing at Axway, perceives BYOD to be the product of employee backlash and circumvention of stringent corporate IT policies that restrict usage of certain technologies. French indicates that BYOD is a "backlash to the backlash" that counteract employees "computing behind the company's back" (French 2012, cited in Caldwell et al. 2012). However, BYOD also brings a number of business benefits including: improved productivity and creativity from a motivated and mobile workforce; sales enablement through increased engagement with customers (Moore and Warner, 2012); and lower IT costs from the elimination of hardware and software purchasing and maintenance expenses from the company budget (Caldwell et al. 2012).

Emerging BYOD Risks and Challenges

However, all new technologies are accompanied by new security challenges (Grabosky, 2007). This literature review addresses the three most frequently identified BYOD risks: data leakage (Gosh et al, 2013; Miller et al. 2012; Morrow, 2012; Wood, 2012), loss of control and visibility (Morrow, 2012; Miller et al. 2012; Thomson, 2012), and ease of device loss (Morrow, 2012; Miller et al. 2012; Gosh and Swaminatha, 2001).

Such information security risks are underpinned by the conflict between Security and Usability. Tokuyoshi (2013) perceives consumerization of IT as a showcase of this conflict. Users, who prioritize usability, select the most appropriate tools for their job, which in turn raises questions about device security and remote access. Thus, different organizations have different 'flavors' of security issues (Tokuyoshi, 2013).

Miller et al. (2012) draws a comparison between BYOD and the introduction of laptops to the enterprise. They believe the security risks and issues associated with BYOD are "largely a replay" of those experienced with laptops. However, they suggest that BYOD is a much harder security challenge because of the larger volumes and ease of loss of devices (Miller et al. 2012). BYOD also introduces the fragmentation of device-level security into the enterprise. Gosh et al. (2013) argued that personal devices have varying degrees of security measures, such as anti-viruses, configuration settings and technical updates; and unauthorized applications may have adverse effects on device and data integrity.

Data Leakage

The storage of critical information assets on employee-owned devices poses a great threat to organizations due to the intended or inadvertent disclosure of sensitive data, such as private customer information and proprietary company information (Miller et al. 2012). For example, sensitive documents downloaded onto a personally owned device is able to be file-shared or stored with minimum or zero security, thus exposing the organization to the risk of data breach.

Loss of Control and Visibility

BYOD introduces new governance challenges that can lead to other serious risks. BYOD presents significant security risks for organizations as they no longer control the device that company data is stored on, hence the enforcement of security policies will be difficult for issues such as data leakage, theft, and regulatory compliance (Miller et al. 2012; Morrow, 2012). Thus, the issue of 'ownership' is at the base of this problem. Organizations have less visibility of the security environment for BYOD compared to a traditional networked environment. Morrow (2012) suggested that there are fewer options to mitigate security risks for unmanaged devices compared to managed devices due to this lack of control and visibility. As organizations increasingly lose control over the security of their terminal devices, employees have a more critical role to play in upholding organizational security. Mansfield-Devine (2012) suggested that organizations must incorporate employees into their security model.

A recent global survey by Fortinet (2011), a world leader in high-performance network security, showed that most employees choose to use their own devices at work despite it being against organizational security policies; and they hold themselves, not the company, responsible for device security issues. Thus, employees can be perceived as the weakest security link in BYOD. Therefore, organizations should consider their employees' needs when developing and implementing BYOD policies.

Managing BYOD devices also present other technical challenges. Firstly, there is a plethora of mobile handsets that are underpinned by various operating systems, which undergo constant technical change and thus get outdated very quickly (Gosh et al. 2013). Secondly, organizations traditionally rely on user-based authentication to approve/deny access, however this must now be architecturally extended to include device-based authentication (Mansfield-Devine, 2012). Thirdly, personal devices can potentially infect the company network with malware (Miller et al. 2012). Armando et al. (2013) also argued that malicious apps can inadvertently be installed as a result of social engineering, as native mobile OS security mechanisms such as 'sandboxing' does not meet corporate security standards, and thus offer limited protection.

Ease of Device Loss

The relatively small size and portability of smartphones and tablets exposes BYOD devices, and the information stored on them, to a higher risk of being lost or stolen (Gosh et al. 2013; Gosh and Swaminatha, 2001). Gartner (2013) found that the weakness of passwords and OS defenses on consumer devices contributes to this risk. To address this issue, the US government and the four major mobile carriers agreed to work together in 2012 to develop a national registry to track all cell phones and tablets. The purpose of this registry is to monitor all devices, and detect and flag missing devices so they can be deactivated (Miller et al. 2012).

Discussion

The consumerization of IT has led organizations to embrace BYOD. Considerable evidence suggests that BYOD brings significant business benefits in terms of reduction in capital expenditure, employee productivity, and work flexibility. However, the information security challenges surrounding the risk of data leakage, device control and management, and ease of loss of devices may outweigh these benefits if not managed appropriately. This is a difficult task to achieve due to the inherent conflict between Security and Usability of BYOD devices. IS strategy must be drafted to achieve a balance between the two. An IS strategy that is too stringent will not

appeal to users while a loosely defined one will not provide the required level of security (French, 2012, cited in Caldwell et al. 2012). Thus, these strategies and the policies that support it must be developed and implemented with the users' needs in mind.

From the literature review, there was no literature that linked the established IS strategies discussed to the new phenomenon of BYOD. Hence, there is no evidence that these IS strategies are effective for managing emergent BYOD security risks. A study by Ernst & Young (2012) found that the gap between the level of IS required to protect against threats, and the actual level of IS measures implemented, is increasingly widening. This suggests that the IS strategies utilized in organizations today are ineffective as security enhancements are lagging behind the rise of emerging threats. It is argued that current IS strategies lack the flexibility, or are too static, to keep up with the dynamism of the mobile threat landscape, and thus BYOD.

In addition to conventional Internet threats, wireless devices bring new dangers that are specific to a mobile medium (Ghosh and Swaminatha, 2001). Hence, the nature of security challenges posed by BYOD is significantly different to traditional corporate devices. The loss of organizational control and visibility of BYOD devices may render a prevention, detection, deception, deterrence, or layering IS strategy to be ineffective in preventing a security breach. For example, a user with a BYOD device can file share confidential corporate information or email a sensitive document. This data leakage arises from the simple fact that BYOD devices can connect to the organization's network but is not managed by its IT department. Thus security policies may not be applied appropriately or enforced. Likewise, the portability of the BYOD devices makes them more susceptible to loss or theft and may inadvertently give access to unauthorized individuals to organization's information or data. Hence, the lack of visibility and control has implications for IS policy enforcement on BYOD devices, which creates a major security loop hole for organizations.

Therefore, it is concluded that no established IS strategies, as they have been implemented in the past, are effective to deal with the emergent security challenges of BYOD.

What can organizations do to Manage BYOD Risks?

One strategy would be complete avoidance by prohibiting BYOD. Some organizations, particularly those in 'fortress industries' where the costs of a security breach outweigh productivity gains, such as government of financial sectors, may choose to retain tight control over their IT environment to prevent exposure to BYOD threats by banning it altogether (Moore and Warner 2013). While this offers a clear cut solution from an information security perspective, changing employee expectations and the high potential business benefits that BYOD brings to the private

organizations does not make it a viable option. In order to harness the power of BYOD, Security and Usability must be coupled in an organization's IS strategy. The question is 'HOW'.

Considering the seriousness of risks posed, BYOD must be encapsulated in an organization's IS strategy to provide an appropriate level of visibility and management, as well as security policy enforcement. As part of this, organizations may consider adopting a Mobile Device Management (MDM) solution.

What is Mobile Device Management (MDM)?

Mobile Device Management (MDM) solutions are a core component of an organization's BYOD security strategy. Albeit not a new technology, MDM is only starting to gain in sophistication due to the encroachment of consumer devices into the enterprise. While Blackberry Enterprise Server (BES) and Microsoft Exchange Active Sync (EAS) have long been used to manage corporate mobile devices, they lacked the maturity to manage non-proprietary devices (Phifer, 2012; Thomson, 2012). Modern MDM technology has been widely implemented by organizations for the management of multi-platform devices (Semer, 2012). MDM They now offer a breadth of security functionalities to allow organizations to maintain "centralized, scalable visibility and control" of BYOD devices (Phifer, 2012; Semer, 2012).

Drawing upon the literature review on IS strategies, MDM systems can be seen as an effective strategic solution for the management of BYOD risks, such as data leakage, loss of organizational control and visibility, and ease of device loss. For example, MDM prevents unauthorized access by reconciling users and devices against security policies using authentication technology. However, if an overly preventive mindset is adopted, this will detract from the usability of the device. Organizations also have the ability to install tracking agents onto devices, thus allowing detection of specific security behaviors that go against defined security policies, such as PIN disablement. This gives organizations visibility of their BYOD environment. As a detection strategy is useless without response (Schneier, 2003), MDM is a good solution as it also couples a response strategy. IT teams can install enforcement policies that allow organizations to automatically respond to detected threats by disabling email or VPN access, and even perform a device wipe (Phifer, 2012; Semer, 2012). The ability to perform remote wiping all corporate data from consumer devices is an effective response strategy for addressing the issue of lost or stolen devices. BYOD presents data ownership issues as the information belongs to the organization however the device belongs to the employees. Some MDMs can address this issue by compartmentalizing employee and corporate data via multiple profiles, thus allowing devices to be decommissioned without harming personal data (Phifer, 2012).

Overall, it is concluded that modern MDM technology is an effective and flexible solution for managing the multi-platform security challenges of BYOD as it encompasses multiple IS strategies in one solution. This is effectively defense-in-depth. However, MDM solutions also exhibit similar weaknesses to conventional detection systems, such as IDS, in that they are static and can only detect known and pre-defined risks. MDM systems do not incorporate self-learning capabilities that renders it useless against unknown or zero-day threats. Schenier (2003) argued that automated systems that have only one response to a specific attack is still considered to be static.

Which MDM Solution?

There are a range of MDM products on the market and selection must be based on the organization's unique mobility needs, use cases and priorities. Phifer (2012) proposes that MDM technologies have two primary focuses: (1) Device and policy management; and (2) Value-add security measures such as authentication and encryption of data containers. Phifer (2012) cited an IDC survey that identified the top two management concerns for BYOD as policy compliance and data security/access. Other concerns include IT support, resource availability, readying mobile applications, setting employees up with multiple devices (Phifer, 2012). Hence, choosing an MDM should not be based on technical security needs alone. An MDM solution must be supported by non-technical elements of information security such as policy and processes. Phifer (2012) suggests that organizations must also "implement desired policies" and the choice of MDM must integrate with "existing infrastructure and support workflows".

BYOD Policy

While MDM is a technical solution for the management of mobile devices and applications, IS policies addressing BYOD usage must also be included in the overall IS strategy to align employees' behaviors and actions towards minimizing the risks associated with BYOD. For example, a security policy will specify what applications can be safely installed on a device, which is then tracked and managed by a security policy manager to identify security violations (Armando et al. 2013). Policies must secure corporate information on mobile devices without detracting from the usability of the device, and thus productivity gained from BYOD. To achieve this, organisations need to understand their employee's motives to maintain control. Frank Andrus (2012), CTO at Bradford Networks, proposes that organizations need to maintain visibility by understanding why employees want to use their personal devices. He also suggests that security policies must be more sophisticated to ensure appropriate organizational control (Andrus, 2012, cited in Mansfield-Devine, 2012).

Employees often find ways to circumvent strict IT policies that they do not agree with (French 2012, cited in Caldwell et al. 2012). From a security perspective, it is argued that users are the weakest link, especially in a BYOD environment. Thus, policies must align with the generational values of employees today. Policies are more effective when employees understand why they must follow them. Hence organizations need to include them in policy-making (Andrus, 2012, cited in Mansfield-Devin, 2012).

Therefore, it is concluded that the involvement of users in the development process of BYOD policies is necessary to obtain user buy-in and compliance and is an effective strategy for converting a weak link to a strong security control. To further increase the resilience of an organization's IS strategy, MDM and BYOD policies should be complemented with other components of the overall IS strategy, such as Staff Education & Training Awareness (SETA) programs to increase BYOD security awareness and governance committees (Thomson, 2012).

Conclusion

This paper has shed light on the established IS strategies and their application, as well as their strengths and weaknesses in securing organizational information. It has also explored the new phenomenon of BYOD and its emergent security challenges, and discusses viable strategies for the mitigation of these risks.

Based on the literature review, it is concluded that no single IS strategy exists for absolute protection against BYOD threats. Hence, defense-in-depth is recommended and multiple IS strategies must be applied. While an MDM solution and a BYOD policy are mandatory components of an organization's IS strategy, their static nature means that there are still inherent weaknesses unless it adopts dynamic capabilities, such as self-learning, to keep up with the fast-changing security challenges associated with BYOD.

This paper contributes to IS personnel's knowledge of BYOD and its associated emergent risks, and suggests options for management of these risks from an information security strategy perspective. As BYOD is a relatively new phenomenon there is has been limited research conducted in this field. This is an opportunity for future research endeavours.

References

Ahmad, A., Maynard, S. B., and Park, S. 2012. "Information security strategies: Towards an organizational multi-strategy perspective," *Journal of Intelligent Manufacturing*), pp 1-14.

Anderson, R. Year. "Why information security is hard-an economic perspective," Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, IEEE2001, pp. 358-365.

Armando, A., Costa, G., Merlo, A., and Verderame, L. 2012. "Securing the "Bring Your Own Device" Policy," *Journal of Internet Services and Information Security (JISIS)* (2:3/4), pp 3-17.

Ballagas, R., Rohs, M., Sheridan, J. G., and Borchers, J. Year. "BYOD: Bring your own device," UbiComp 2004 Workshop on Ubiquitous Display Environments2004.

Caldwell, T. 2012. "Prepare to fail: creating an incident management plan," *Computer Fraud & Security* (2012:11), pp 10-15.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The value of intrusion detection systems in information technology security architecture," *Information Systems Research* (16:1), pp 28-46.

GHOSH, A., GAJAR, P. K., and RAI, S. 2013. "BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES," *Journal of Global Research in Computer Science* (4:4), pp 62-70.

Ghosh, A. K., and Swaminatha, T. M. 2001. "Software security and privacy risks in mobile e-commerce," *Communications of the ACM* (44:2), pp 51-57.

Grabosky, P. N. 2007. *Electronic crime*, (Pearson Prentice Hall.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM* (54:6), pp 54-60.

Liu, S., Sullivan, J., and Ormaner, J. 2001. "A practical approach to enterprise IT security," *IT Professional* (3:5), pp 35-42.

Mansfield-Devine, S. 2012. "Interview: BYOD and the enterprise network," *Computer Fraud & Security* (2012:4), pp 14-17.

McFadzean, E., Ezingeard, J.-N., and Birchall, D. 2007. "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Information Review* (31:5), pp 622-660.

Miller, K. W., Voas, J., and Hurlburt, G. F. 2012. "BYOD: Security and privacy considerations," *IT Professional* (14:5), pp 53-55.

Moore, C., and Warner, J. 2013. "Industry Contexts And Constraints Diversify Approaches To Bring-Your-OwnTechnology," December 13, 2012.

Morrow, B. 2012. "BYOD security challenges: control and protect your most sensitive data," *Network Security* (2012:12), pp 5-8.

Niehaves, B., Köffer, S., and Ortbach, K. Year. "IT consumerization under more difficult conditions: insights from German local governments," Proceedings of the 14th Annual International Conference on Digital Government Research, ACM2013, pp. 205-213.

Park, S., Ruighaver, A. B., Maynard, S. B., and Ahmad, A. Year. "Towards understanding deterrence: Information security managers' perspective," Proceedings of the International Conference on IT Convergence and Security 2011, Springer2012, pp. 21-37.

Park, S., and Ruighaver, T. Year. "Strategic approach to information security in organizations," Information Science and Security, 2008. ICISS. International Conference on, IEEE2008, pp. 26-31.

Porter, M. E. 1997. "WHAT IS STRATEGY?," Harvard Business School Publication Corp., pp. 156-157.

Qian, Y., Fang, Y., and Gonzalez, J. J. 2012. "Managing information security risks during new technology adoption," *Computers & Security*).

Schneier, B. 2003. *Beyond fear: Thinking sensibly about security in an uncertain world*, (Springer.

Straub, D. W., Goodman, S. E., and Baskerville, R. 2008. *Information security : policy, processes, and practices / Detmar W. Straub, Seymour Goodman, Richard L. Baskerville, editors*, (Armonk, New York : M.E. Sharpe, c2008.

Sveen, F. O., Torres, J. M., and Sarriegi, J. M. 2009. "Blind information security strategy," *International Journal of Critical Infrastructure Protection* (2:3), pp 95-109.

Tirenin, W., and Faatz, D. Year. "A concept for strategic cyber defense," Military Communications Conference Proceedings, 1999. MILCOM 1999. IEEE, IEEE1999, pp. 458-463.

Tokuyoshi, B. 2013. "The security implications of BYOD," *Network Security* (2013:4), pp 12-13.

Wang, G. 2005. "Strategies and Influence for Information Security," *Information Systems Control Journal* (1).

Wood, A. 2012. "BYOD: The Pros and Cons for End Users and the Business," *Credit Control* (33:7/8) 12//, p 68.

Yeniman Yildirim, E., Akalp, G., Aytac, S., and Bayram, N. 2011. "Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey," *International Journal of Information Management* (31:4), pp 360-365.

"Key findings from Ernst & Young's 2012 global information security survey 'Fighting to close the gap.'," *AUDIT AND RISK*:9) //, pp 10-11.

"Fortinet(R) Global Survey Reveals 'First Generation' BYOD Workers; Pose Serious Security Challenges to Corporate IT Systems; Over 1-in-3 Respondents Would Contravene Company Policy Banning the Use of Personal Devices at Work or for Work Purposes," (available at https://ezp.lib.unimelb.edu.au/login?url=https://search.ebscohost.com/login.aspx?direc

t=true&db=edsnbk&AN=13F8576D147A10C0&scope=site).
Gartner, Inc “Bring Your Own Device: BYOD is here and you can't stop it.” http://www.gartner.com/technology/topics/byod.jsp

Author/s:
DEDECHE, AHMED;Liu, Fenglin;LE, MICHELLE;Lajami, Saeed

Title:
Emergent BYOD security challenges and mitigation strategy

Date:
2013

Citation:
Dedeche, A., Liu, F., Le, M., & Lajami, S. (2013). Emergent BYOD security challenges and mitigation strategy. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33340