Review Article ISSN 2639-944X

Journal of Medical - Clinical Research & Reviews

BYOD, the Advancement of Enterprise and Mobile Civilization: Challenges and Prevalence

Sadiq Abdulkarim[1], Abubakar Ismail Muhammed[2*], Samaila Kasimu Ahmad[2] and Muhammed Ibrahim[2]

[1]*Faculty of Science and Information Technology, Daffodil International University Dhaka, Bangladesh.*

[2]*Faculty of Computing, Nigerian Army University Biu, Borno State, Nigeria.*

[*]Correspondence:
Abubakar Ismail Muhammed, Faculty of Computing, Nigerian Army University Biu, Borno State, Nigeria.

Received: 07 Jun 2022; **Accepted:** 10 Jul 2022; **Published:** 15 Jul 2022

Citation: Abdulkarim S, Muhammed AI, Ahmad SK, et al. BYOD, The Advancement of Enterprise and Mobile Civilization: Challenges and Prevalence. J Med - Clin Res & Rev. 2022; 6(7): 1-7.

ABSTRACT

The industries keep expanding its horizon, modern computing on the forefront of the labor market and its industrial reformations. As these modern computing backbones extends, hence the need for more subordinating devices. This paved the way and allow for the resounding evolution of the modern computing as against the stone-aged and analogues era. As the world keeps up its nocturnal submersions, so also the need for a corresponding drift in the directions of mobile computing. The trends and evolution of mobile computers such as smartphones and laptops has bring about a swift turnaround in the fields of computing. Users are able to move freely with their devices and use it extensively to utmost satisfactions. Mobile computers play vital and essential roles in our lives. Users use these devices almost everywhere they are allowed such as homes, workout hubs, beaches, tourist grounds, workplace etc. Daily usage of these devices tends to create some sorts of mutual relationships between the users and the devices. These relationships range from comfortability, familiarity, ease-of-use etc. As these devices tend to assume an appreciable fraction of our life's endeavors affecting our lives in diverse ways, it tends to find its way in almost all aspects of our lives. These essences brings about a new trend where employees are allowed to bring their own devices and use it in all aspect of their work deliverables. The concept that describes this trend is known as "Bring your own device" BYOD.

Keywords
a&w-p model, BYOD, Corporate enterprises, Mobile computing, Security triad.

Introduction (BYOD)

The concept of bring your own device (BYOD) has been around for a while, even though it wigs actually started surfacing around 2003, it was until 2011 that it finally begins to poke its head around [1] one would say it has definitely come to stay. One would then ask, what exactly is the concept, BYOD all about? Various researchers in the field have invariably defined this concept [2]. Defined BYOD as the use of employee-owned devices to access enterprise contents and the enterprise network. The surging-force BYOD as an academic-industrial discipline is inverting on the edges and apexes of modern computing cannot be minutely emphasized because of the evolution of modern computing. For the purpose of this paper, we define BYOD as the deliberate action of enterprise centered upon allowing employees to come along with them to work their personally owned devices to be use in accessing enterprise data contents and network resources with the sole aim of carrying out their respective workloads/tasks. In this paper, we will be discussing.

BYOD as a concept, we looked at the patterns drawn by the evolutional trails of this emerging concept, also, we adder sing the challenges such as security, impacts based on the job demands and job resources model JD-R MODEL and possible mitigating solutions to these upraising challenges, we also looked at the benefit, prevalence, current status and future expectations of this concept. We also propose elevated models that address, louds etc. the supposed concepts. From the very onset, companies, firms and enterprises are responsible for defining and controlling the technological infrastructures used by workers and employees within the domains of their corporate environments, meanwhile in

the recent times, there have been some debrides of change around here, these firms no longer dictates what and how devices are used. This is propelled and instigated due to the progressive spread of mobile devices. These bring about the birth of a new aphorism "Technology brings work to home and home to work.

Evolution, Trends, Prevalence and Status of BYOD

The ovum BYOX (bring your own anything) study showed that 67.8 percent of smartphone-owning employees use theirs for work, 15.4 percent of those do so without the IT support unit knowledge and 20.9 percent of those do so in spite of an anti-BYOD policy already put in place. Over the past decades, there has been a virtual boost in the information technology architecture of BYOD [3].

BYOD STATs

On the very verge of getting a head start as to the trailing nature of BYOD and to get a better understanding of the impact of this new trend, we worked through some credible statistical data from credible Sources.

Table 1: BYOD Transition from 2016 to 2018 [4].

Countries	Change in Percentage
United States of America	65-77%
Asia	62-74%
Africa	34-53%
Russia	58-63%

- At least 87% of companies worldwide center their attention on their employees coming over with and using their personal devices to gain access to enterprise network and contents [5].
- At a time, length ranging around 2016, 2/5 companies had an already predefined policy that entertains BYOD [5].
- Platforms that entertain and harbor BYOD are on the verge of hitting $367 billion upfront 2022 as against its resounding figure of $30billion in 2014 [6].
- Using employee's own devices (BYOD) instead of company own devices reduced overall cost of about $500 thousand annually [7].
- A study carried out by prominent researchers Frost and Sullivan shows that by using devices of high mobility, employees tend to save for themselves up to 58 minute each day and correspondingly increase their productivity by 34% [8].

One will get to ask the question, what exactly does the future have in stock as about this new trend? As mentioned above, BYOD platforms are setting up monuments that aid their quest of striking close to $367 billion by 2022. Well, that is indeed a bright future for BYOD. From all indications, this trend has come to stay for long. It obviously will continue to find favor in the eyes of employees and enterprises alike. Who grasp the opportunistic nature of using the very devices one is more familiar with? Who wouldn't embrace flexibility in their place of work? The freedom of having to play around and being able to access and work from just about anywhere in the world. Nonetheless, it seems from all indications more likely that enterprises will work towards having to set up their own policy as about BYOD in a way that agrees and yields to the conventional/existing way of doing stuff in the enterprise.

Implementing BYOD

On the verge of implementing BYOD, an enterprise has an appreciable number of options to pick from, this of course must be inline and agrees with the policies that defines both the internal and external structures, working mechanisms etc. of the enterprise.

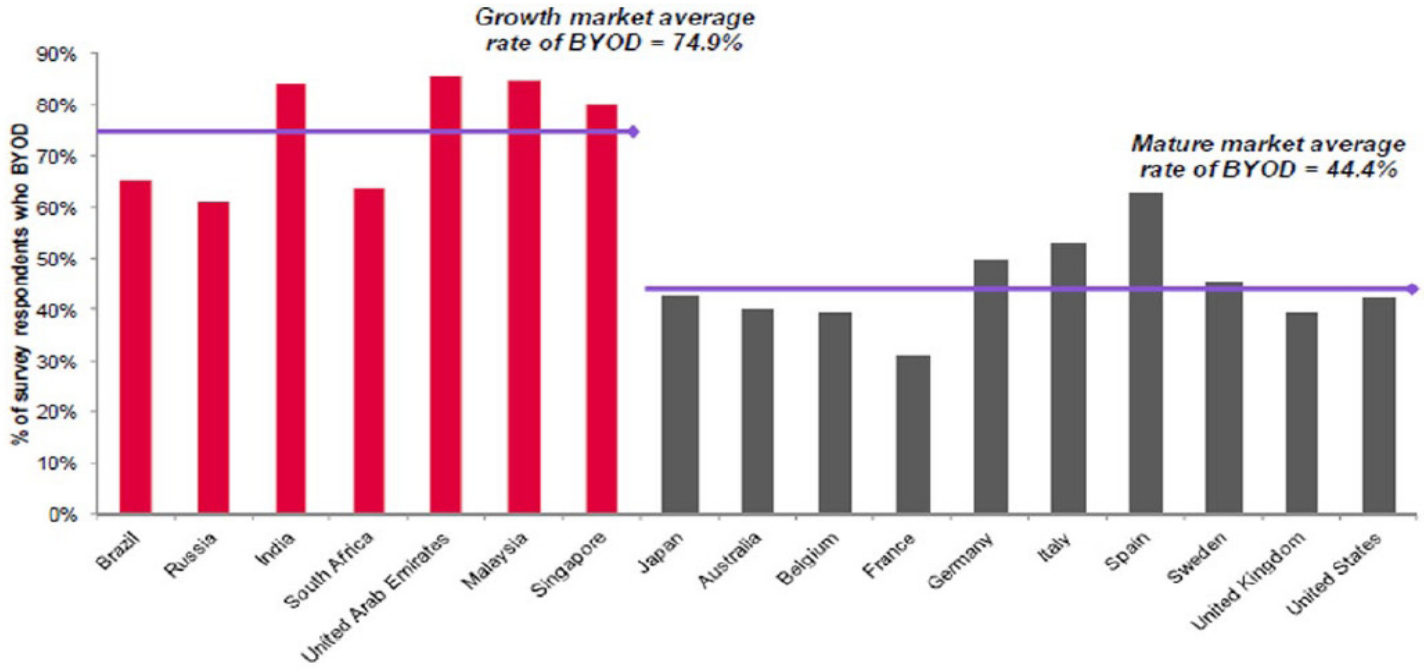

Figure 1: Level of BYOD development in both emerging economics and developed economics [10].

These options could be based on the amount of content that a given worker could access with his/her device, time of assessments, and nature of contents and mode of assessment. For example [9] was able to identify a key number of obvious issues relating to the use of a rather direct or straightforward method of manually checking of employees smart PCs and devices in a periodic or sporadic fashion for the presence of any form of security threats and hence taking the necessary step of preventing eventual security breaches. First, this could be time consuming, as there might be a good number of employees and devices that might also need such checking. In the course of this paper, we outlined some strategic key points based on the nature of the data or contents. The nature of contents could take one of the following forms:

a. **Confidential Content (sensitive contents):** while certain information, contents or data needs to have restrictions on its usage, there are contents that are meant to remain only within the scope of the enterprise and its workers. These types of contents are known as CONFIDENTIAL CONTENTS. Restrictions are only made to individuals outside the enterprise's domain. As such, every worker or employee within the framework of that enterprise is liable to access and use these types of contents based on his/her work descriptions.

b. **Ultra-sensitive contents (protected contents):** even within the framework of a given enterprise, there are certain types of data or contents that are restricted to just highly placed, critically picked and high-profiled individuals. This cadre of individuals is allowed access to these types of contents based on their positions, nature of work deliverables etc. While these types of contents must exist only within the enterprise domain, certain workers/employees are not liable to the assessment of these contents. Often, the nature of these types of information when tempered-with, or accessed by wrong hands or leaked to the outside world usually poses some sorts of highly significant threats (lives and properties), loss of enterprise's status etc.

c. **Public-based contents (non-sensitive contents):** contents that when eventually, either deliberately or in-deliberately released to the public will not in any way harm the integrity of either the enterprise or the clients of which the contents is directed at. In fact, these sets of contents are made purposely for the public consumption.

d. **Access-Write Protected contents (a&w-p model):** in the supposed a&w-p model of the nature of contents and information piece, there are certain types of contents that are not just only restricted to the enterprise itself, but are restricted to individuals that reside in and outside the enterprise. This means that even highly privileged, highly authoritative power holders of the enterprise are not liable to accessing or even modifying this type of content. In order to achieve and implement a&w-p model, certain types of encryption algorithms must be adopted. These mathematical algorithms must ensure that the contents are restricted to the participating individuals (sole owners of the contents). Many cryptographic experts in the field of cryptography have invariably defined the term cryptography and encryption algorithm. At the course of these research paper, we define an encryption algorithm to be sets of mathematical functions and standing schemes that has the capabilities of converting or making an intelligent or meaningful piece of content looks more of a gibberish than a complex piece, in a process known as encryption in such a way that no one or anyone (be it the enterprise workers and authorities) upon interception of these piece of content cannot make any sense or rather comprehend the meanings behind the contents and hence restricted from accessing, using or modifying it, and can only appear meaningful to individuals with the key of sole ownership in an antithetical process known as decryption. An example of such type of scheme could be seen in the supposedly popular cross-platform internet-based messaging software, WhatsApp and its end-to-end encryption schemes or its social media messaging counterpart signal.

As with regards to the above outlined end-points, an enterprise could adopt one of The following Possible options as listed below; of course contents that fall under a&w-p model are not regarded in the options below:

i. ***Unlimited access to unlimited*** contents could be given to users with a high authorization index. Here the listed individuals could access all contents at any point in time. Whether within or outside the Enterprise's domain. These individuals could work from home, work-out hubs, public and private transits etc. with their own devices and could access from of course outside the network of the Enterprise the contents.

ii. ***Unlimited access to limited contents***. Here the listed employees could access the Enterprise contents and network from just about anywhere and anytime but are restricted to just certain predefined contents. These limitations are necessary especially when the said employee is not authoritative enough to gain access to highly confidential information.

iii. ***Limited access to unlimited contents.*** Here the said individuals are allowed to use their own personally owned devices to access just about any form of enterprise networks and data but are restricted to certain times of access. These could take forms such as predefining the time that the employees are liable to content assessment or where the employees could make the assessment. This is more of a state and time affair

iv. ***Sparser/loose-limitations*** could be attributed to certain picked employees. Again, these sets are handpicked based on the nature of their work deliverables. Here the type of contents, time of assessment, where the assessment should be made, how it should be made etc. are critically predefined. For example, an employee is allowed to access the logbook of phone users in the district but cannot make the assessment during break hours or during work hours or from his/her home. These could also take other states and forms such as defining the type of contents that an employee could access using his/her personally owned devices and those that must be only accessed using the Enterprise's IT department based devices.

v. ***Supervised access***. Here, either access could be limited or unlimited contents could be either limited or unlimited. However, the key point of this type of implementation is that the IT support unit gains mutual controls over employees' personal devices. This of course cannot happen without a prior agreement between the said employee and the IT support unit in question. The support unit could make dictations such as preventing employees from storing contents on local storage or from using a personal device that is not registered with the unit.

Impacts, Benefits and Future Expectations of BYOD

Research shows that using one owned device to carry out tasks can save employees and workers an averaging time length of about 58 minutes each day and correspondingly increase users or employee's productivity by 34%. Debates as about the supposed increased efficiency of employee's notion as inclined to implementing BYOD has been around for a while. Researchers such as [11] argued, "There's yet to emerge any well-proven theory or group of theories that leads to the notion of work positivity and satisfaction based on the use of personally-owned devices in carrying out work deliverables". Meanwhile [12] argued counter-intuitively by outlining five concepts that play a direct impact on job performances. These concepts include self-responsibility, IT competency, functionality, work-life overlap and work satisfaction. People's mental faculties are more at ease when using their devises instead of employer's [13].

One of the benefits of implementing BYOD, which cannot be ignored, is the direct effect of an appreciable reduction-in-burdens on the parts of the enterprise itself. As new devices are introduced in the market, each with an inscribed added benefit and functionalities, Enterprise on the verge of moving alongside the trends of things get to upgrade to these new devices. This has many implications, workers might be inept and lack competency with these devices, it is of course the duty of the enterprise to train the workers in order to get more conversant with these conventional office devices. Also, based on existing office devices and tools, the enterprise will have to take it upon themselves to introduce and train new employees through the working mechanisms of this devices which on most occasion requires man-resources (resource persons either within or outside the enterprise), time, money and a fractional delay in what need to be done and deliverables that need to be delivered in that period of time. The trends on BYOD were able to address these supposed problems. First, it minimizes the costs of first having to buy these devices and the hectic work of having to teach supposed employees how to use these devices if bought. With BYOD, employees whom by nature have high tastes for new devices and the zeal to always move alongside the drifts made by the information technological eras tend to, beforehand acquire these devices, get used to them, and get acquainted with them. In addition, will always when offered with the options, opt to use their own devices.

Needless to say, often the enterprise are more Worried and concerned about the security aspects when it comes to implementing BYOD, employees on the other hand tend to be more concerned about their conveniences when it comes to using their very own devices to carry out their tasks as well as the privacy they deserve and expects in terms of personal information stored in their devices. Outside these, employees will always go for their personally owned devices when offered the choice of choosing their working devices, this boosts their motivational energy and helps them work and stay productive. Businesses/enterprises tend to benefit tremendously when BYOD is implemented as they get to reach out and have access to their employees at any given point in time.

Challenges of Implementing BYOD

Implementing BYOD comes along with lots and loads of benefits. As stated above, it is a double-edged sword. While it offers all the benefits it has in stock, it could turn around and send its poignant edge cutting through your flesh thereby inflicting you with an unbearable pain, in fact some individuals argue that it's a "bring your own danger" and not device. An enterprise implementing BYOD tends to benefit so much from it. While this is true, it would be illogical for one to shy away from of course the obvious glitches, problems and challenges that come along with this trend. Alongside other possible challenges, security stands out as the most daunting of all challenges associated with implementing the said trend. The reasons as to why this is true are not far-fetched. Security has always been in the forefront of modern computing, people, organizations, companies and large-scale enterprises are hyper-cautious when what is tabled at the table of reality is security. The significance of having personal, confidential pieces of data and information-compromised results in a rather disastrous, closely followed by outrageous responses by affected parties. For example one of the most popular and widely known attack in the history of mankind; a stuxnet attack on Iranian grid systems destroying many infrastructural architectures such as the centrifuge systems [14]. This attack leads to a tremendous loss of millions. It is widely believed that a worker having his USB drive inserted in one of the supposed critical systems initiated this attack. The impact of this attack also spans and extends towards affecting the industrial infrastructure of the NATANZ nuclear facility.

In the course of this research paper, we outlined the possible challenges faced in the real world with of course real-world scenarios. These points are closely followed by possible suggested strategies aimed at mitigating this supposed glitch.

Table 2: Ratio of Individuals Who Maintain Erasing Data from Lost Devices.

Age	Number	Collected data: Ratio of Individuals who Maintained Erasing Data as against the Others.
18-20	9	09:00
21-23	6	06:00
24-28	6	05:01

Security attacks on Enterprise network: prior to what [15] claimed => loss or theft of mobile devices tend to be the most hazardous and biggest risk that any business or corporate enterprise could face at the verge of BYOD implementation, security attacks are in fact the most consequential and daunting risk. The analysis is

simple and concise, the coincidences attached to the possibilities of a lost mobile device falling into the hands of someone who could or have interest in consuming the piece of information found in the devices is thin. How we were able to draw this conclusion from of course credible inferences is not beyond us. At the course of this research, we carried out a systematic analysis extracting our data from individual resource persons. This survey was carried in a higher institution environment, based in Borno state, Nigerian. Ages of participating parties ranging from 18-28. 21 pupils were analyzed. The survey had a questioning tag related to what one tends to do with a found mobile device of which the founder has an interest in keeping or using for personal gain such as selling-off, keeping for personal use etc. and from the data collected, 94% of these surveyed individuals have zero or imperceptible interest in the contents of the device, in fact the first thing they tend to consider is ripping the devices off whatever contents they might contain.

From the above, we are able to draw conclusions that the biggest risk an enterprise could face from implementing a BYOD is being victims of a directed security attack. For any directed attack made to an enterprise by any adversary or attacker, all pieces of information obtained are valued and used. This means that for any successful security attack, the enterprise surfers one or more hits as opposed to loss of devices that could possibly fall into the hands of someone with zero interest in it.

Security attacks could take several forms when it comes to an enterprise implementing BYOD. An enterprise could surfer hit, the success of the hit could be traced to an employee. An attacker could exploit the BYOD implementation of an enterprise, seek out a weak link which could be the mobile device of the employee who has either limited or unlimited access to the enterprise network and contents.

Possible security attacks that an enterprise could surfer could be summarized in the following:

- Attack on Confidentiality: We define confidentiality in terms of a security attack as one of the triad of the triangle of cyber security as an effort centered upon making sure a sent message coming from a source gets to and only to the intended recipient with zero interception. Attack on confidentiality entails having an adversary eavesdropping on the lines of the enterprise and having an info, content or resources redirected to unauthorized persons. Examples of attacks on confidentiality include eavesdropping, data mining, rerouting etc.
- Attack on Integrity: taking the position of been one of the key elements in the triangle of cyber security, we define integrity in this context to be an effort centered upon making sure a piece of information say M intended for a recipient say R from a source S in the course of relaying do not take a different form say Q altered by an adversary say A for the sole purpose of causing a misinterpretation of some sort or stirring up and upsetting a soup of mutual understandings between the two authorized parties. Examples of these kind of attacks that an enterprise could surfer include data injections, data alterations etc.
- Attack on availability: attacks on availability entails denying authorized users piece of information, data or contents by stealing, destroying or blocking it. This is dangerous to enterprises' relationship with their clients because no enterprise will appreciate upsetting their clients and thereby breaking the bridge of mutual understandings. Examples of this type of attack include call flooding, call/session hijacking, and distributed denial of service (DDOS) attack.

Preventing security attacks on a BYOD-related architecture

- o Setting up good security policies that define possible security standards that should be followed by employees.
- o Having mobile devices frequently checked by the IT Department to ensure all possible needed security patches are made.
- o Frequent/non-stop usage of security related software, firewalls, and proxies such as virtual private network (VPN). etc.

Data Loss/leakage: Scenarios where individuals get to lose certain data stored on the local storage of their devices is common, regardless of whether or not the contents lost are confidential or non-confidential, whether or not it could or could not be useful to an outsider who by chance bumps to it. Data can be lost or leaked either due to a break in hardware architecture/components say storage systems or loss of device itself. Either way, this could make a significant impact to the enterprise in question. Possibility could exist that the contents of the lost devices are highly confidential to the enterprise and having these contents in the wrong hands could cause great havoc.

Ways to prevent data loss/leakage include:

- **Cloud computing adoption/implementation:** with the evolution of cloud computing and cloud storage, users get to store up or back up their data in some sort of cloud storage service. This way, loss of devices does not call for loss of data as these contents could easily be looked up and recovered from the signature cloud storage of the enterprise.
- **Mobile device management (MDM):** MDM services are strategically developed to mitigate some of the arising issues associated with mobile devices. MDM has the sole ability of critical issues based on areas like inventory management, application distribution and usage. For example in the case of a lost device, a service Requiring MDM could assume the abilities of been able to remotely gain access to the lost devices and either retrieve or destroy the data that are resident on the device.it could also function as to monitoring of the registered device for any form of malicious threat and sorts.

Non-compliance with BYOD Policies: For a successful Implementation of BYOD and an extensive utilization of what the trend has come to offer and what the enterprise could achieve from implementing it, certain requirements/policies are therefore outlined. Policies including employee's proper code of conduct, actualization of memorandum of association etc. All these are laid down policies that are meant to ensure a swift and successful implementation of BYOD. However, situations exist where professional ethics, yielding to managerial constitution,

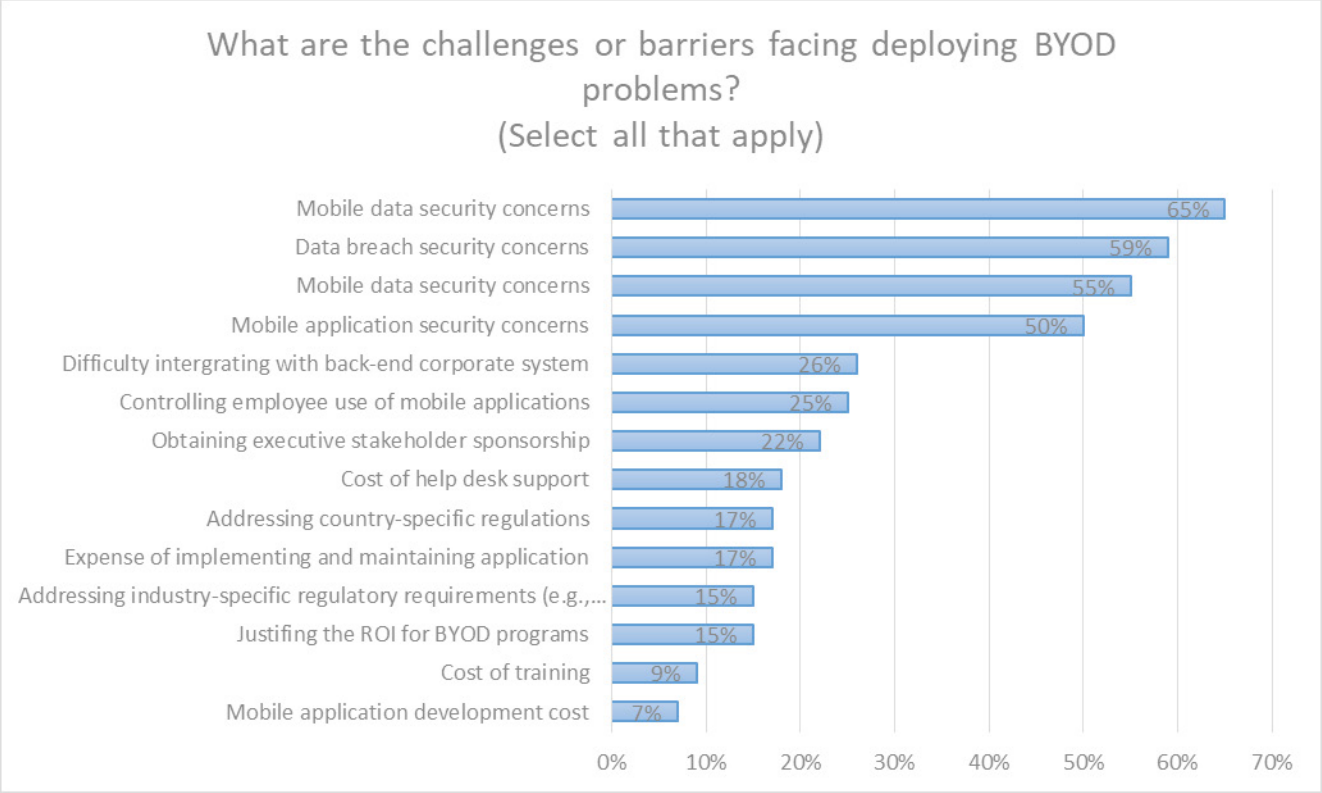

Figure 2: BYOD challenges with security concerns at the top [16].

succumbing to constitutional employees find it hard to comply with them. For example, it would be very difficult for users to comply with policies that require employees to use their personal devices to carry out work deliverables but never to use it for personal activities, as it could be distracting and hence bring about a decrease of productivity. While this is true, employees might find this strange and feel their freedom of using their own devices freely is being ripped apart. It seems almost pragmatically infeasible and inevitable to successfully convince employees of total abstinence from the personal use of their own devices. In addition, there exist issues where sacked employees stubbornly walk out of the Enterprise's complex having enterprise data residents on their devices even when there exist laid down policies that kick against it. Reasons could be a means of revenge.

Ways of mitigating Non-compliance issues.

- Control plans should be laid down by the IT Department before BYOD implementation agreement. This might take the form of setting standards that aid immediate retrieval of contents when need be.
- Security teams should be laid down to control procedures that are backed by legal agreement. This might require legal jurisdictions to play a vital role of addressing critical issues when there is a bridge of agreement or policy.

Conclusion

One could start with the packages BYOD has cometh to offer, one could likely also start with the issues and challenges associated with this trend, whatever the case might be, BYOD when implemented using the right tools (policies, implementations, procedures, arts etc.) and the right paradigm will bring about a turnaround and an evolutionary skew-ness (skewing to the right-hand side) in modern computing. Effortless researches made by effortless researchers on the verge of seeking out effortless ways of paving the right tunnels and canals of BYOD down the aisle of modern civilization. New strategies keep swooping in and out and as a result, BYOD happens to be successful in finding a place in the market. While we cannot ignore the upsides of implementing BYOD, we still cannot shy briskly away from its downsides. Sorting out strategic procedures to aid a maximization of its upsides and a corresponding minimization of its downsides are the sole objectives of present contemporaries/researchers. From the outcome of the survey carried out in the course of this paper, direct attack is clearly the height treat BYOD implementation can face compare to stolen devices, given that 94% of the candidates that participated in the survey maintain erasing the device instead of keeping the date/information on the device will be their priority.

References

1. Leavitt N. Today's mobile security requires a new approach. Computer. 2013; 46: 16-19.
2. Deloitte. Understanding the bring-your-own-device landscape by invitation only. 2013; 5-22.
3. French A, Guo C, Shim J. Current status, issues and future of bring your own device BYOD Communications of the Association for Information Systems. 2014.

4. Forbes. The future of byod statistics, predictions and the best practices to prepare for the future, retrieve on Jan 21. 2019.
5. https://www.prnewswire.com/news-releases/syntonics-top-predictions-for-byod-and-enterprise-mobility-in-2016-300190987.html
6. Johnsson A. Growth of byod proves it's no longer an optional strategy. Beta News. 2017.
7. Cisco. Bring your own device, Cisco IT Insights. Cisco Public. 2014.
8. Suby M, Dickson F. The 2013 ISC 2 global information security workforce study Frost and Sullivan in Pertnership with Booz Allen Hamilton for ISC2. 2015.
9. Li X, Hsieh JJPA, Rai A. Motivational differences across post-acceptance information system usage behaviors an investigation in the business intelligence systems context Inf Sys Res. 2013; 24: 659-682.
10. Ovum. BYOD an emerging market trend in more ways than the one Logicalis Business and Technology Working as One. 2012; P2.
11. Giddens L, Tripp J. It's my tool I know how to use it A theory of the impact of BYOD on device competence and job satisfaction. Twentieth American Conference on Information Systems. 2014; 1-8.
12. Niehaves B, Köffer S, Ortbach K, et al. Towards an IT consumerization theory A theory and practice review Working Papers ERCIS-European Research Center for Information Systems. 2012.
13. Abdulkarim S, Binord F. The psychological effect of bring your own device BYOD OIRT Journal of Information Technology. 2021; 1: 6-9.
14. Rosenbaum R, Clark R. Who was behind the stuxnet attack? Smithsonian magazine. 2012.
15. Al-harthy K, Shawkat W. Implement network security control solutions in byod environment Conference Control System, Computing and Engineering ICCSCE IEEE International Conference. 2013.
16. Olalere M, Abdallah MT, Mahmod R, et al. A review of bring your own device on security issues, SAGE Open. 2015.