Blog Post: the rise of BYOD

“Bring Your Own Device” is a rising trend where employees utilise their own devices within a workplace to access resources like an email server. In this brief post, I look at BYOD, its benefits, implications for business, and security and privacy issues.

Benefits

Van Der Heijden (2004) identifies two rather insightful benefits of information systems: “hedonic benefits” and “utilitarian benefits”. The terms reflect why we use information systems: because of the intrinsic *benefit* we derive from their usage. “hedonic” refers to enjoyment or happiness obtained. In contrast, “utilitarian” refers to functional benefits often related to financial rewards. Such benefits often guide users to determine the inherent risk required to use a system or even how much their data remains private. (Dincelli et al., 2017)

A BYOD strategy offers many benefits, such as reducing the purchase and maintenance cost of devices—the burden shifts onto employees—reducing device theft and increasing employee preference. Also, employees tend to look after their own devices better than the organisation’s (Oktavia and Prabowo, 2016). Allowing employees to utilise whichever device best suits the task leads to greater flexibility and allowing them to complete tasks anytime or anywhere (Singh, 2012). Organisations that adopt BYOD policies also positively impact their social attractiveness when recruiting potential employees (Weeger et al., 2016). Another study found that BYOD employees work an extra two hours daily (Deyan, 2020 and generate approximately $350 of value per employee.

Security

A security concern of BYOD is that organisations do not have complete control over how their data is accessed, stored or even where it is stored. Employees automatically assume that data stored on their devices are secure without considering authentication measures at the location of storage (Blizzard, 2015). Another security concern relates to insecure or vulnerable apps on the device, which increases the risk for data leakage of sensitive company information.

According to Dincelli et al. (2017), privacy and security are not yet clearly delineated but are closely related. For instance, “privacy is the individual’s right to be left alone from intrusion”. At the same time, “information security” is the focus of protecting data from hackers. In this way, privacy and security are intertwined and difficult to separate because many systems handle data about people. Therefore, it is not always possible to “be left alone” and protect from intrusion that is left alone.

Adopting BYOD policy ensures each device complies with relevant legal regulations when using the devices to interact with an organisation’s confidential data. Such policies must consider areas such as:

- ***Networks.*** The IT department of an organisation IT department bears the most responsibility for ensuring sound security concerning BYOD. The IT department must address data protection, anti-malware, updates, device detection, password policies and other issues such as access to Wi-Fi, Bluetooth, VPN and network monitoring tools. Here, IT must align with the strategies of the organisation (Ratchford et al., 2021)
- ***Security Policies.*** BYOD requires effective, coordinated policies and governance. Nevertheless, such policies are often inconsistent across departments, leading to security failures. Furthermore, in this regard, the *user* plays an active role in information security since they become responsible for unwanted incidents on their devices (Zahadat et al., 2015).
- ***Stolen Devices.*** Losing a personal device is not an experience we wish to encounter. Suppose that a device (such as a smartphone) contained sensitive company information. The impact of loss grows exponentially to the value of the data. For this reason, organisations can consider Mobile Device Management (MDM) and Mobile Application Management (MAM) solutions. MDM registers and approves devices with access to company information. MAM manages the use of applications installed on the device based on the user’s role.

Securing information systems is about protecting the perceived *beneficial nature* derived from an information system’s data. Threats, internal or external, to that benefit pose enormous risks and potential financial losses to an organisation. In order to secure BYOD devices, a policy may call for the need to require physical access to the devices and even PINs to secure them. However, such access requirements can be interpreted as a direct invasion of privacy.

In the following graph by HelpNetSecurity (2021), the top five concerns companies expressed relates to data leakage, vulnerable apps, stolen devices, unauthorised access and malware.

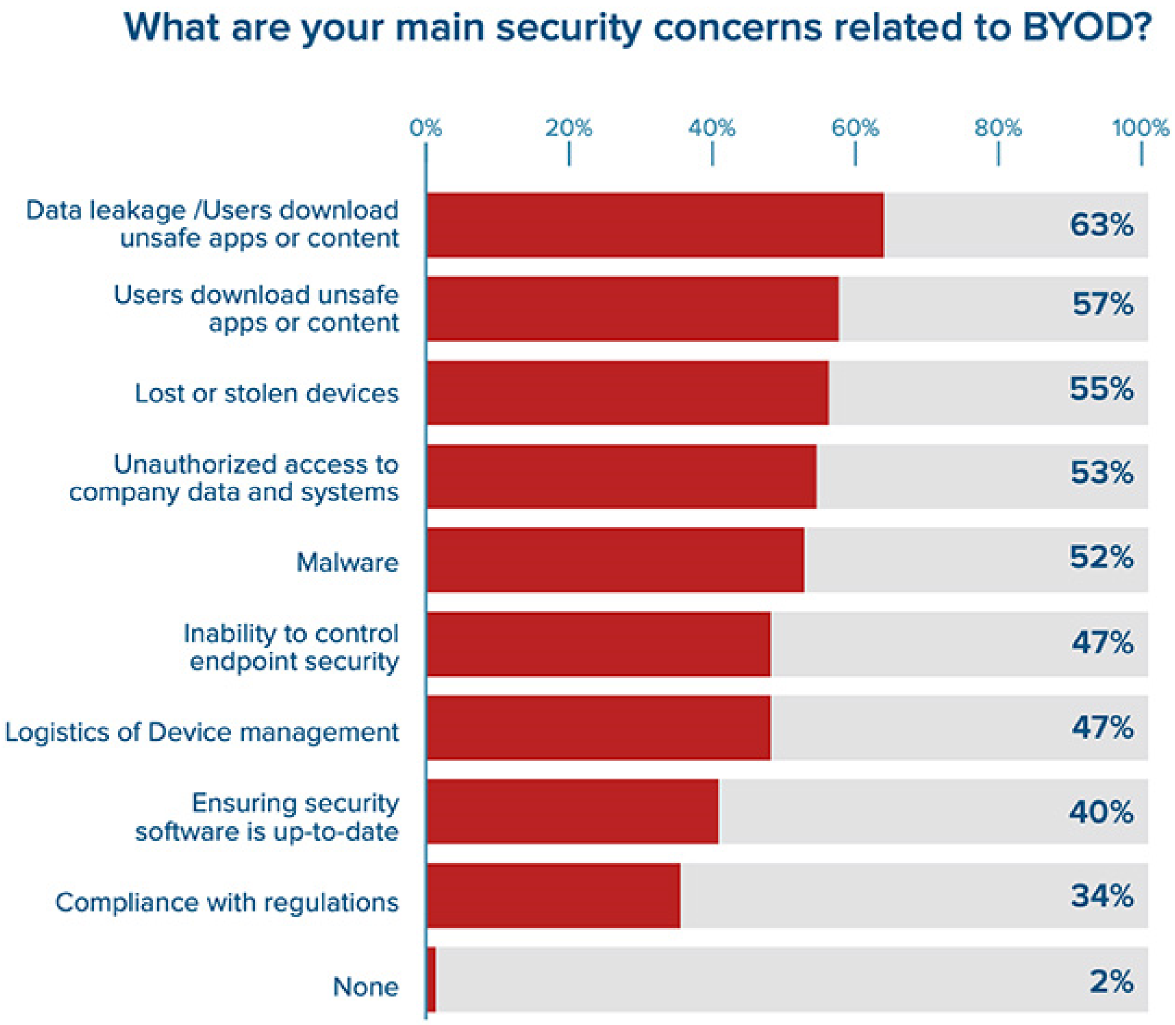

Figure 1 Security concerns of BYOD (HelpNetSecurity, 2021)

Privacy

Smith (2017) provides a good analogy regarding privacy by using the example of "Joe", who walks through one's home. "Joe" gains access to different parts of the house that contain information he should not access usually. According to law, "Joe" commits no criminal activity because the *intention* of accessing rooms and any data is not an action *explicitly targeted* at the homeowner. The homeowner did not necessarily lay down rules for what may or may not be accessed. Similarly, the saying "Access to information is not wrong; it is *what is done with it* that matters" summarises the actions of "Joe".

Nissenbaum (2009) states, regarding privacy, (emphasis added, mine)

> *"We have a right to privacy, but it [is] neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in*

> *which our **expectations about the flow of personal information** are, for the most part, met"*

While it is challenging to clarify the nature of privacy, Smith (2017) considers privacy a concept whose boundaries shift based on situation, culture, and even personal preferences. Gold (2015) notes that sixty-one percent of workers believe their personal information must remain private in the context of BYOD. For example, the phishing scam at Presbyterian Healthcare Services (HealthcareDive, 2019) exposed social security numbers, birth dates and health plan information via an email account phishing attack.

As BYOD usage grows, employers increasingly will encounter claims of rights because employees own their devices and pay for connectivity (claims often skewed in favour of employers). BYOD policies must, therefore, clearly understand the difference between organisation ownership and personal ownership over the devices.

Implications

Most certainly, BYOD has a positive impact on employees' productivity, who save on average, 81 minutes per week. Such time savings translates to roughly £1000 every year in device and software maintenance costs. Because the top BYOD concern is data leakage and vulnerable apps, organisations may have to look to artificial intelligence (AI) to uncover malware or other software vulnerabilities. Cloud services, too, may play a valuable role in provisioning BYOD devices. For example, Microsoft Office 365 supports APIs to facilitate mobile app management; Apple has introduced the concept of User Enrolment; and, Google has created Work Profiles to secure work data in a separate container on personal devices. Since BYOD facilitates a work-from-home culture, organisations may need to consider reimbursement plans for employees who utilise their own devices

Conclusion

The traditional model of leveraging an organisation's infrastructure, using trusted hardware from trusted suppliers, is slowly making way for a new paradigm of infrastructure: personal work devices. The trend will grow in the coming years 5G (and shortly, 6G) networks start supporting the real-time connectivity of any device. The BYOD market's estimated compounded annual growth rate is around 15% between 2021 and 2026 (Chang, ND). Moreover, in terms of support for BYOD (especially among SMEs), BYOD has 88% support in some countries and 69% within the US market (ResearchAndMarkets, 2021).

BYOD is a natural extension of an organisation's existing infrastructure and collection of interacting information systems. It may seem overwhelming, but the relentless march of new technology does not slow for organisations that fail to adapt. With such massive support for employees and BYOD, success inevitably depends on incorporating these edge-infrastructure devices, including clearly defining a BYOD strategy, policies for risk mitigation and access control boundaries.

References

Blizzard, S. (2015) Coming full circle: are there benefits to BYOD?. *Computer Fraud & Security*, 2015(2):18-20.

Chang, J. (ND) 44 Basic BYOD Statistics: 2021 Market Share Analysis & Data. Available from https://financesonline.com/byod-statistics/ [Accessed on 23 Jul 2021].

Deyan, G. (2020) 43+ Stunning BYOD Stats and Facts to Know in 2021. Available from https://techjury.net/blog/byod/ [Accessed 23 Jul 2021]

Dincelli, E., Goel, S. & Warkentin, M. (2017). Understanding nuances of privacy and security in the context of information systems. *Twenty-third Americas Conference on Information Systems.* Boston, 2017.

Gold, J. (2015) "BYOD users worry employers can't keep private data safe". Available at https://www.networkworld.com/article/2946157/mobile-security/byod-users-worry-employers-cant-keep-private-data-safe.html [Accessed 22 Jul 2021]

HealthcareDive (2019) Phishing scam at Presbyterian exposes 183K patients' data. Available from https://www.healthcaredive.com/news/phishing-scam-at-presbyterian-exposes-183k-patients-data/561745/ [Accessed 23 Jul 2021]

HelpNetSecurity (2021) BYOD adoption is growing rapidly, but security is lagging. Available from https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/ [Accessed on 23 Jul 2021]

Nissenbaum, H. (2009), Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford, CA.

Oktavia, T. & Prabowo, H. (2016) Security and privacy challenge in Bring Your Own Device environment: A Systematic Literature Review. *International Conference on Information Management and Technology:*194-199. IEEE.

Ratchford, M., El-Gayar, O., Noteboom C., & Wang Y. (2021) BYOD security issues: a systematic literature review. *Information Security Journal: A Global Perspective*. DOI: 10.1080/19393555.2021.1923873.

ResearchAndMarkets (2021) Virtual Private Server Market – Growth, Trends, COVID-19 Impact and Forecasts (2021 – 2026). Available from https://www.researchandmarkets.com/reports/5239391/virtual-private-server-market-growth-trends?utm_source=BW&utm_medium=PressRelease&utm_code=gcqfbq&utm_campaign=1461078+-+Global+Virtual+Private+Server+Market+Growth%2c+Trends%2c+and+Forecasts+Report+2020-2025+-+Small+and+Medium-sized+enterprises+(SMEs)+to+Show+Enhanced+Association+towards+VPS+Offerings&utm_exec=chdo54prd [Accessed on 23 Jul 2021]

Singh, N., (2012) BYOD genie is out of the bottle–“Devil or angel”. *Journal of Business Management & Social Sciences Research*, 1(3):1-12.

Smith, W. P. (2017) “Can we borrow your phone? Employee privacy in the BYOD era”, *Journal of Information, Communication and Ethics in Society* 15(4):397–411.

Weeger, A., Wang, X. & Gewald, H. (2016). IT consumerisation: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems* 56(1):1-10.

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