bsi.

...making excellence a habit.™

Bring Your Own Device (BYOD)

An information security and eDiscovery analysis

A Whitepaper

Executive summary

Organizations often turn to Bring Your Own Device policies (BYOD) for their mobile device capabilities. Employees purchase the device they like and are comfortable with, and the organization pays the bills. However, data breaches and other incidents are not often expected but can be pricey for the company.

A BYOD agreement or policy is usually the minimum agreement but the risk of data being leaked by mobile devices can be high. To help mitigate this, BSI would recommend having the appropriate software in place to manage mobile devices. While the implementation of this software is important, it is essential that it is managed and updated in an appropriate and timely manner or it can lose its protective value. The question every organization has to ask itself is, *"when all the risks are tallied up, is BYOD really as beneficial for organizations as it appears?"*

Risks and challenges

Accessibility and ownership challenges - the human factor

Employees are primarily the weakest link as far as information security is concerned and mobile devices are no different[1]. Nowadays mobile device users must sign terms and conditions, which they very often skip to the end and accept any terms necessary to download the latest version of software, or to get the most popular application on their device.

If an employee decides to start a new job in a different organization and wants to bring his or her device with them, it may prove difficult to separate personal and work data on the device. From a technical point of view, the folder structure and organization is not as defined as it would be on a PC and even if the employee agrees to format the device (which would essentially wipe the device), work data could be contained in a backup that could potentially be at their disposal. If the device has device manager software it may be possible to disable certain access but it can be difficult to guarantee that all contact details or email attachments are permanently wiped from the device. Employees come and go, and some do so more amicably than others. Some employees will cooperate, and others will not be as happy to part ways with a phone they purchased themselves which stores their personal data, such as: conversations with friends and family, the stats of their weekly run, their synced pictures and files etc.

Research shows that some employees feel that a BYOD policy could be detrimental to their work-life balance[2], but this research also shows that employees who are encouraged to access work-related documents on their personal device still do so in their own personal time. When the lines between our work and our personal life are blurred, mobile security can get complicated and data management (and its discovery) is not as straightforward as we would hope.

Security, preservation and privilege review

Many organizations have BYOD policies, but unfortunately most do not have strict policies which they apply in an effective manner. That type of BYOD management can result in an organization being subject to an unnecessary level of risk. With the new General Data Protection Regulation (GDPR) being enforced on the 25th of May 2018, organizations will have to place more focus on the fact that mobile devices are data sources which are in scope for subject access requests and other relevant GDPR requirements.

In addition to the security risk that could materialize, in

1 "[…] over 95 percent of all [cyberattacks] incidents investigated recognize "human error" as a contributing factor." IBM Security Services 2014 Cyber Security Intelligence Index, https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

2 https://www.egnyte.com/blog/2014/05/byod-blurring-the-lines-for-work-vs-personal-time/

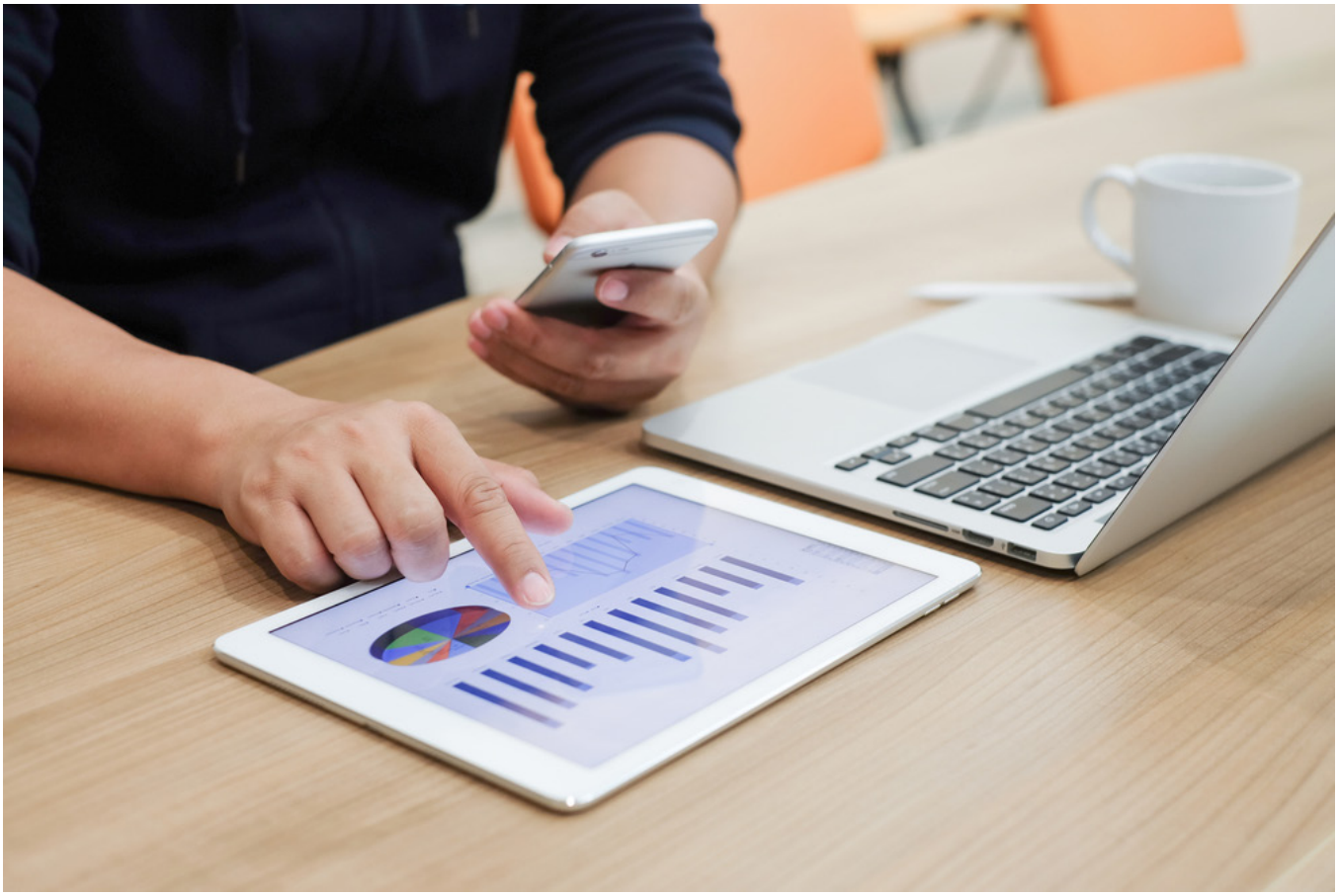
eDiscovery, an employee's lack of cooperation can be a hurdle in the collection process. Even if employees cooperate, the question remains, what if that employee is now an ex-employee with a new position in another company and uses that same device to access other data? This will create a whole new battle between companies as they will not want their data to be accessible to the other. This could result in long delays and legal discussions, which in turn becomes costly and prevents access to the data to be investigated in a timely manner. Organizations can request certain actions when an employee leaves, such as: requesting that a backup is wiped, or that specific file types and email or contacts are deleted. An IT department can choose to trust that the individual has complied with their request or ask that they do it for the individual. However, depending on how the device is set up and whether or not there is a Mobile Device Management (MDM) tool in place, it will be difficult to distinguish between work and personal text messages or work and personal chat messages.

If a device is used for both work and personal purposes, the volume of data contained in that device would likely contain vast amounts of data that is irrelevant to the eDiscovery request. As this personal data is likely to be hidden or mixed in with the work-related data, it will take resources to strip the potentially relevant data from these devices, therefore increasing the costs of the legal review and the volume of the data to be processed and hosted by the service provider. In terms of volumes, a mobile phone's storage usually ranges between 16 GB to 128 GB. If we were to convert this into hard copy it could range from 1,036,512 pages to 8,292,096 pages.[3]

Individuals do not expect to be the subject of an eDiscovery request when they sign up to a BYOD policy and they probably do not envisage their device and all of their personal data contained within (web search history, lists of websites and apps) to be inspected at any point in time.

So, is it really more cost-effective for a company to have a BYOD policy if they run the risk of their data being leaked, not being able to access the data on the devices in a timely manner and having to run a review of additional amounts of potentially non-relevant data in addition to a privilege review?

3 Conversion done on the basis of Average pages/gig of Microsoft® Word® Files (https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf)



Solutions

Although there is no one-stop-shop solution to BYOD security, there are a number of measures organizations can implement to help mitigate the risk.

Remember that data stored and accessed from mobile devices is still data we have to control and manage

GDPR is quite clear in setting out the stall that the organization is responsible for the security of its data wherever it is located – on premise or in the cloud. Data stored on mobile devices is no different. Organizations must take responsibility for this data and put the necessary defensive measures in place.

Have a clear BYOD policy and keep it up to date

An extensive analysis of the BYOD policy and strict mobile device and application management are paramount to support the adequate and reasonable protection of company data. Employees need to know where they stand in regards to usage rules and guidelines.

Once a clear and concise policy has been developed, one key element is communication of this policy and seeking wide spread adoption and understanding. Employees need to feel engaged in the process and given the chance to provide feedback and make suggestions in order to be fully engaged.

Many organizations make the mistake of simply developing the policy and leaving it up to employees to educate themselves. This nearly always results in low adoption rates and breaches of the rules.

Acquire Mobile Device Management (MDM) software to implement the policy

As technology advances and devices are added to the policy, it is vital that companies seek assistance to keep their policies up to date by implementing MDM and MAM tools.

Investing in built-in eDiscovery solutions may also prove useful for an organization when faced with eDiscovery requests. This will allow the organization to have more power over their data and manage it in a more effective way.

Using archiving tools, data monitoring or built-in eDiscovery tools in cloud-based products will allow for searching within emails and easy extraction of the results which can then be reviewed by the appropriate people. These solutions would also avoid any realisation that implementation of deletion policies may have resulted in a loss of data which had not been envisaged by the IT or Legal department.

Therefore, planning for the worst and hoping for the best is important: the above solutions can be extremely beneficial for the protection of the organization and keeping costs as low as possible when collecting data and will allow the organization to maintain more control.

Create awareness among employees to ensure they comply and are proactive as opposed to reactive when issues arise

Training employees on information security and cybersecurity best practices is a great way to raise awareness on what security measures can be put in place to avoid, to the greatest extent possible, any vulnerability coming from a mobile device. There is training software in the market that offers modules specific to mobile device security which can train employees on what precautions they can take when using a mobile device for work purposes.

It's important to educate rather than punish employees for mistakes made. Human error is best combated with education awareness and just-in-time coaching. Mobile users are particularly susceptible to threats such as phishing as once out of the working environment, users can often neglect their security responsibilities if accessing non-work related content.

We recommend a constant, ongoing and evolving education series as opposed to an annual box-ticking exercise that is less likely to be effective.

Be aware of the risks (ransomware, data leakage, hacking) and ensure you have methods to remediate these

Although the ideal situation is to avoid a cyber incident, being prepared for one in the event of it occurring is a

vital piece of the defensive jigsaw. A calculated Incident Response plan is needed so that the company knows how to respond and who is responsible for what, in the event of a breach.

Mobile security is a vital component of this plan. If a mobile device was breached, would you know how to investigate this and report on what information has been compromised on this device? Can you answer definitively what protection methods you have in place to protect your devices?

Find a security partner

Find a security partner to assess the policies and implementation periodically to ensure they are up to date and your organization's data is secure.

Continuous risk assessments and testing will ensure that the organization stays secure and the BYOD policies are being followed. Find an accredited security partner and work with them to ensure all policies are up to date and fit for purpose. Try to avoid a progremme of ad hoc exercises and implement a continuous improvement methodology.

Conclusion

BYOD is not an easy subject for organizations to tackle and takes careful consideration, intricate planning and adequate investment to manage properly. It is especially difficult as IT security teams must tackle the risks posed by human error and mitigate these with education of the user and adequate technologies for their company's needs with the added difficulty of mobility added to the mix. However, if all of the elements outlined in this paper are considered, organizations can mitigate these risks to acceptable levels and leverage the overwhelming benefits presented by embracing the mobile world.

Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 345 222 1711

Call IE: +353 1 210 1711

Email: cyber@bsigroup.com

Visit: bsigroup.com