COM 416 BYOD Research Paper

Matthew Neadly

Joshua Adams

04 December, 2016

Saint Leo University

Technology is constantly evolving, becoming more powerful yet contradictorily smaller at the same time. In the span of a few decades we went from desktop computers to phones a fraction of the size; that have more processing power and functionality. The impact technology has had on society is almost indescribable. People rely on smartphones and the internet in such a way that they cannot function without them. This level of dependence has prompted many institutions to harness the technologies their students or employees already carry with them. Bring Your Own Device or BYOD is the policy whereby businesses allow their workers to perform company tasks on their personal machines (phones, tablets, etc.). The mentality behind this strategy is that users are more comfortable with devices they purchased and know how to use. Allowing the user to use a device he or she already has saves the company money; since it no longer has to purchase as many devices as it once did. Theoretically productivity can also increase because adaptability hurdles are bypassed. BYOD is not without its faults, as security professionals know, more devices in an environment just means more potential threat vectors and risks to confidential information. In order to mitigate and prevent the dangers associated with BYOD one needs to analyze it from a multi-layered and comprehensive viewpoint.

The biggest trap companies fall into is complacency, throughout this course we discussed several instances where breaches occurred and the litigation and damages associated with the hacks were exponentially worse; than the costs would have been; had the business been willing to adopt higher security standards. Before an enterprise decides to incorporate personal machines into the workplace they need to define a clear and incredibly detailed policy that not only makes sense to the powers that be, but also is clearly communicated to the staff; so that they not only can utilize the technologies, in the ways the organization intends, but also so that they realize what can happen to their personal data. The second you use a privately owned device in the workplace the data and information stored within are property of the company. If certain secrets or other relevant documents are housed on your phone and the company decides it needs to wipe the device; you can kiss your photos and other personal elements goodbye (Gaff, 2015). This may seem extreme but unfortunately the potential impact that phone could have on the business if it went rogue is so catastrophic these policies need to be adhered to.

Wiping data is only part of securing the organization; the devices the company allows to access its network need to be limited as well. New threats and malware are being developed daily. A device that was secure a month ago may no longer be secure, the older a device gets the more time hackers have had to tear into it, identify what makes it tick, and understand how to gain control of it. Allowing machines into your business that you know pose enhanced danger to not only the continuity of the mission but also to the customers who gave their information to you and expected you to keep their P.I.I. (Personally Identifiable Information) secure. If an employee wishes to use his or her gadget in the workplace that is fine provided it reflects the standards outlined in the regulations and procedures. Companies are playing with fire when they gamble on cyber security. The mentality is frustrating to say the least, the owners would think you were crazy if you told them not to put a lock on their door or implement a security system on the physical premises. Yet they staunchly resist safeguarding electronic assets; which in the modern era are sometimes more valuable than the resources stored in the building. Criminals go where the money is, hacking is becoming easier and more accessible; as professionals on the internet train others, for a price, and malicious software tools are becoming both more sophisticated and simpler to acquire. To ignore the severity and debilitating problems this could have on your livelihood is not just foolish it is shameful.

Attacks can come from literally anywhere, what makes the war against hackers so frustrating is the fact that the malicious hackers are always ahead of the honorable ones. The myriad of angles, methods, and tools the attacks can come from make them virtually impossible to predict. As professionals we need to monitor advancing trends in the field, keeping privy to not only the hardware and software emerging, but also how data thieves are infiltrating enterprises. What techniques seem to divert them towards weaker prey? No organization no matter how secure they appear, or how iron clad their policies are, is impervious to a breach. That makes our jobs that much more integral to the sustainability of the institution. Whether it be DDOS, Social engineering, Malware whatever the case they are all damaging (Yuan, 2016). The multifaceted approach of protection is crucial if one wants to even have a chance of weathering this digital storm of intrigue and skullduggery we find ourselves in.

Various theoretical concepts for smartphone security are being thrown around amongst the computer science community. Whether it be SpotMal a software that shelters businesses from malignant applications but simultaneously places reverence on the importance of user privacy (Gudo, 2015). BYODroid another software that tries to defend that which seems so indefensible in this climate of cyberwarfare (Armando, 2013). DroidARM which tries to restrict the applications a device can download in the workplace (Oluwatimi, 2016). PriPARD that also want to secure corporate environments from the harsh realities we currently face (Gheorghe, 2013). The point is everyone can agree that data security is necessary and that BYOD, while cost cutting to a company, simultaneously exposes the business to more attacks. What they disagree on is how the solution should be remedied. There is no silver bullet, no miracle cure that can vanquish all your problems.

The degree to which cyber security forces you to think is insane. Threats exist everywhere. Is an attack coming from an independent entity, a county, an extreme political sect. Then even after you determine who is conducting the barrage; which could take a very long time depending on the complexity of the assault you still need to make sure you keep the business alive and close off the entry point to prevent further complications. The odds are definitely with the assailants, even if they only get a fraction of the data you possess they can still make a profit. Look at ransomware the FBI recommends paying it once it gets too far embedded into the machine. Cryptography definitely can help prevent data theft because information you cannot understand is useless to you but now the devices are being manufactured with Trojans and defects inserted directly into the hardware itself (Van Dijk, 2015). Never assume you are immune from attacks or that they could never happen to you, because your business is too large or too small they can and if trends continue they will. Security professionals need to petition the upper echelon of companies and educate them of the chaotic situations they are unwittingly setting themselves up for. Communication is key to actually achieving change sitting behind a computer is no longer enough to be effective in the field you need to convey information and messages to those who can actually influence the company and persuade them to take the steps required to dodge calamities.

Just when you think you have the information secure, a new technology comes along and turns the whole organization on its head. But this technology is not going away; Pandora's Box has already been opened, schools, businesses they are all adopting these devices (Berger, 2016). We cannot afford to stick our heads in the sand and hope for the best. We need to continue fighting to secure the futures of the institutions and people associated with them. If this paper does anything I hope it serves to educate those reading it that the computer world is one of the last frontiers we as a species have yet to truly understand. New threats, technologies, and methodologies are being discovered and conceived all the time. The need to constantly learn and adapt to the changing landscape can feel frustrating and understandably so but that doesn’t make the consequences associated with breaches and hacks disappear. They are here to stay regardless of how we feel. Good eventually triumphs over evil this is true in the material world as well as the cyber one. By keeping tabs on the tools and dangers emerging from digital space we can shift the battle in our favor.

References

Ammeloot, A., Benyon, D., & Mival, O. (2015). Design principles for collaborative device ecologies. *Proceedings Of The 2015 British HCI Conference On - British HCI '15*. http://dx.doi.org/10.1145/2783446.2783598

Armando, A., Costa, G., & Merlo, A. (2013). Bring your own device, securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13*. doi:10.1145/2480362.2480707

Armknecht, F., & Guajardo, J. (2014). Proceedings of the 4th International Workshop on Trustworthy Embedded Devices - TrustED '14. doi:10.1145/2666141

Berger, H. & Symonds, J. (2016). Adoption of Bring Your Own Device in HE & FE Institutions. *Proceedings Of The The 11Th International Knowledge Management In Organizations Conference On The Changing Face Of Knowledge Management Impacting Society - KMO '16*. http://dx.doi.org/10.1145/2925995.2926027

Gaff, B. M. (2015, February). BYOD? OMG! *Computer,* 10-11. doi:10.1109/MC.2015.34

Gheorghe, G. & Neuhaus, S. (2013). POSTER: Preserving privacy and accountability for personal devices. *Proceedings Of The 2013 ACM SIGSAC Conference On Computer & Communications Security - CCS '13*. http://dx.doi.org/10.1145/2508859.2512500

Ghinita, G., & Rughinis, R. (2014). An efficient privacy-preserving system for monitoring mobile users. *Proceedings of the 4th ACM conference on Data and application security and privacy - CODASPY '14*. doi:10.1145/2557547.2557559

Gudo, M., & Padayachee, K. (2015). SpotMal. *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists - SAICSIT '15*. doi:10.1145/2815782.2815812

Huang, H., Zhu, S., Chen, K., & Liu, P. (2015). From System Services Freezing to System Server Shutdown in Android. *Proceedings Of The 22Nd ACM SIGSAC Conference On Computer And Communications Security - CCS '15*. http://dx.doi.org/10.1145/2810103.2813606

Huang, H., Chen, K., Ren, C., Liu, P., Zhu, S., & Wu, D. (2015). Towards Discovering and Understanding Unexpected Hazards in Tailoring Antivirus Software for Android. *Proceedings Of The 10Th ACM Symposium On Information, Computer And Communications Security - ASIA CCS '15*. http://dx.doi.org/10.1145/2714576.2714589

Katara, S. & Ilavarasan, P. (2013). Mobile technologies in e-governance. *Proceedings Of The 7Th International Conference On Theory And Practice Of Electronic Governance - ICEGOV '13*. http://dx.doi.org/10.1145/2591888.2591955

Kumar, R., & Singh, H. (2015, February 06). A Proactive Procedure to Mitigate the BYOD Risks on the Security of an Information System. *ACM SIGSOFT Software Engineering Notes, 40*(1), 1-4. Retrieved September 04, 2016, from http://dl.acm.org.ezproxy.saintleo.edu/citation.cfm?id=2693231

Lyon, C., & Osterman, M. (2014, November 02). Security BYOD: Be Your Own Defense. *SIGUCCS '14 Proceedings of the 42nd Annual ACM SIGUCCS Conference on User Services,* 29-32. Retrieved September 04, 2016, from http://dl.acm.org.ezproxy.saintleo.edu/citation.cfm?id=2661176

Martinelli, F., Mori, P., & Saracino, A. (2016). Enhancing Android permission through usage control. *Proceedings of the 31st Annual ACM Symposium on Applied Computing - SAC '16*. doi:10.1145/2851613.2851797

Oluwatimi, O. & Bertino, E. (2016). An Application Restriction System for Bring-Your-Own-Device Scenarios. *Proceedings Of The 21St ACM On Symposium On Access Control Models And Technologies - SACMAT '16*. http://dx.doi.org/10.1145/2914642.2914645

Twinomurinzi, H. & Mawela, T. (2014). Employee perceptions of BYOD in South Africa. *Proceedings Of The Southern African Institute For Computer Scientist And Information Technologists Annual Conference 2014 On SAICSIT 2014 Empowered By Technology - SAICSIT '14*. http://dx.doi.org/10.1145/2664591.2664607

Van Dijk, M. (2015). Hardware Security and its Adversaries. *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices - TrustED '15*. doi:10.1145/2808414.2808422

Vorakulpipat, C., Polprasert, C., & Siwamogsatham, S. (2014). Managing Mobile Device Security in Critical Infrastructure Sectors. *Proceedings Of The 7Th International Conference On Security Of Information And Networks - SIN '14*. http://dx.doi.org/10.1145/2659651.2659742

Wang, H., Zhang, Y., Li, J., Liu, H., Yang, W., Li, B., & Gu, D. (2015). Vulnerability Assessment of OAuth Implementations in Android Applications. *Proceedings Of The 31St Annual Computer Security Applications Conference On - ACSAC 2015*. http://dx.doi.org/10.1145/2818000.2818024

Yuan, X., He, W., Yang, L., & Simpkins, L. (2016). Teaching Security Management for Mobile Devices. *Proceedings Of The 17Th Annual Conference On Information Technology Education - SIGITE '16*. http://dx.doi.org/10.1145/2978192.2978227