PAI PRIVACY ASSOCIATES INTERNATIONAL LLC

# Bring Your Own Device

*IAPP KnowledgeNet Detroit*

*November 5, 2013*

# Purpose

- Provide a forum to discuss implications of use of employee owned devices “BYOD” in the workplace
- Discuss competing priorities and concerns in creating and implementing BYOD policies
- Provide information for use in assessing existing BYOD practices and consideration of enhancements from the session learning.

# Methodology

- Use created factual scenarios as the basis to engage in open discussion
- Ask participants to role play
- Ask for comments from all as we proceed

# Mega Co

Mega Co has manufacturing and retail operations throughout the US and is considering international expansion. The company maintains an active and successful e-commerce site where customers may purchase products using credit and debit cards which are processed in-house. Mega Co's insurance subsidiary sells personal protection insurance policies to individuals through Mega Co's retail locations, the subsidiary's insurance agents as well through a network of independent insurance agents.

# Mega Co - Continued

Mega Co provides its sales and marketing staff with company owned mobile devices. At the same time Mega Co is consolidating its existing data processing centers and plans to take convert some of its in-house applications to similar applications available in the "cloud" to save money. Mega Co has a policy prohibiting employees from using their own mobile devices for company business despite a rather vocal desire by its employees to use their own mobile devices. This is especially true from the field force that seems to be constantly on the road working to acquire suitable building sites as part of the international expansion plan.

# Mega Co - Continued

Ms. Bigbucks, Mega Co. CFO, has decided it makes good business makes sense (dollars and cents) to reconsider the existing prohibition and allow employees to bring and use their own mobile devices for work. In addition, she has an uneasy feeling several key people are already using the devices despite the policy and if the workforce finds out it will not be pretty.

# Mega Co - Continued

Ms. Bigbucks, also knows there is work in "doing BYOD right". She needs a well thought-out plan before committing to the change. And after a few minutes of reflection she know exactly what to do. . . .

# “Congratulations, I have a project custom made for you”

You are the Chief Privacy Officer at Mega Co., a well respected manufacturer and mass market retailer. In addition to your existing crushing workload, you have been tasked with a new project. You can hardly wait to put into practice all the wonderful things you have learned from participating in the super duper Detroit IAPP KnowledgeNet group and from attending IAPP conferences.

# Plan Ahead

- Conduct risk analysis
- Involve the key stakeholders
- Develop a BYOD strategy
- Create appropriate policies
- Engage and train employees
- Enforce policies

# Wednesday

# Wednesday Facts

- Victoria, VP facilities development, is boarding a plane to return to the US from Outer Mongolia after a successful business trip. Since she had been on the road for a month is really looking forward to getting back home in time to relish the long weekend. Her trip has been very successful in locating sites and potential partners for Mega Co. The last thing she has to do is complete performance evaluations for her team. Fortunately, she had the foresight to get copies of the employment files from her friend in HR before she left on the trip and had them downloaded to her company-issued tablet (VPs get the best toys). Now it is just a matter of some paper work on the first leg of the homeward bound trip and she is done.

# Wednesday Facts

Tom (HR employee) not wanting to take his laptop home over a long weekend  and especially since he is also taking off Thursday and Friday , downloads the current quarterly benefits files to a flash drive so he can work on them at home on his home computer over the weekend.

# Thursday

# Thursday Facts

After watching his son play in the local junior high school football game Tom decides to do a little work and then begin relaxing for the weekend. He downloads the files from the flash drive to his home computer, gets to work, wraps it up, and calls it a night. After completing the tasks and before heading off to lullaby land, he re-copies the revised data to the flash drive and places the flash drive in his coat pocket.

# Thursday Facts

Victoria is still traveling and is a bit worst for the wear. She completed the performance reviews last night and thought she placed her tablet in her carry-on bag, in fact, she was certain she did. Image the surprise of the cleaning crew member who found a tablet computer in the seat back pocket; he quietly slipped the tablet into the trash bag and then took it home.

# Friday

# Friday Facts

Tom meets up with Sally for lunch. They keep their coats on the chairs and enjoy a nice meal. After lunch Tom runs a few errands at the local mall. He is exhausted and heads home. When he gets home he remembers one small task he needs to finish for work, so he boots-up the home computer and goes to get the flash drive from his coat pocket. To his dismay and discomfort the drive is not there. He searches the house and can't find it anywhere. He decides it is lost so he just goes and retrieves the file he left on the home computer and gets to work. He finishes, finds a spare flash drive to use, and once again puts the "new" flash drive in his coat pocket.

# Friday Facts

Victoria realizes the tablet is missing and calls the airline to see if someone turned it in. No luck. She does not have a separate listing of company personnel so she tries reaching the Mega Co main desk. Unfortunately, all she reaches is the voice response unit and she decides to leave a voice mail hoping someone would get the message over the long weekend.

# Friday Facts

Sally, an employee of a Mega Co competitor (and unscrupulous one at that) is having lunch with Tom. She and Tom are rumored to be friends with benefits. Sally is been tasked by her company's management to gain "business intelligence" about Mega Co's expansion plans. She knows Tom has access to sensitive company information. At lunch with Tom, he mentions he has work to do and he is carelessly fiddling with a flash drive as he talks -- as if it contains the work project. Sally is certain there is something of value on the drive. When Tom is not looking she lifts the drive from his coat pocket. Tom is clueless.

# Saturday

# Saturday Facts

Tom enjoys the rest of the weekend.

# Saturday Facts

Victoria arrives home and did not hear from anyone. She calls Mega Co security to report the lost tablet

# Saturday Facts

Susan, the Mega Co security person on duty, is having a bad day. She is fighting with her significant other over something silly and is getting grief from a couple of her co-workers. Susan answers a call from Victoria. She hears stories over and over, somebody (this time a mucky-muck) loses her new electronic toy. It's just another lost device, besides no one really seems to care. She never hears anything back from anyone after filing the lost device reports.

# Saturday Facts

After hanging up with Victoria, she dutifully completes a lost device report form on *paper* and puts it in the "out" box. It is late and she is clocking out. Besides, to save energy she is required to turn off devices not being used and she has already turned off her assigned desktop computer. Since it is Saturday she concludes there isn't anyone around to see an email report-- even if she filed it. Susan is certain it's no big deal and it can wait until Monday when folks are back in the office.

# Saturday Facts

Sally uploads the data from the Mega Co flash drive she stealthily obtained from Tom's coat pocket. She is hoping she is getting company secrets she will use to promote her career. Instead she finds financial information about Mega Co employees, including all the data necessary to engage in some "account takeover" financial gain. Sally knows a few people who will pay for this type of data. She does not know what they do with the data and really does not care -- as long as she is paid.

# Sunday

# Sunday Facts

- Tom enjoys the rest of the weekend.
- Early morning Sally sells the data to her “friends” and enjoys the upcoming week with extra money to spend.

# Monday

# Monday Facts

Tom returns to work. No mention is made of the lost flash drive. As a member of the HR staff he is well aware of the policies on BYOD and concludes no one will know and if he reports the loss he could be subject to disciplinary action.

# Monday Facts

Susan starts her day with a slight tinge of guilt. On her way home Saturday she heard a radio report about ID theft from stolen and lost devices. She started thinking if she was right in submitting the report from Victoria on paper instead on an electronic form.

# Monday Facts

To put her mind at rest and soothe her slightly guilty feeling, Susan pulls the report (which was still sitting in the out-going mail tray) and calls Maggie, her supervisor. Susan informs Maggie about the VP's lost tablet. After hanging up, she feels much better and gets back to work protecting the facility from unwanted intruders.

# Monday Facts

Maggie, Susan's security supervisor at Mega Co, just got off the phone with Susan and has reviewed the lost device report Susan submitted on behalf of Victoria. Since Victoria is a VP, Maggie knows she should let others know, after all a VP is someone important. Trouble is, Maggie is uncertain whom to call. She looks for and finds a printed copy of the company telephone directory and looks for someone in IT to call.

# Monday Facts

Maggie calls the IT Security Department. Gerald, a front line supervisor in the IT security department answers. Maggie relays the information about the lost tablet. Gerald seems distracted, as though he is being interrupted from doing something important. Having completed the information transfer, Maggie hangs up the phone and gets on with her day.

# Monday Facts

Jose, manager of the HR benefits help line, is working the early shift. It was a quiet until a few minutes ago. Then it seemed as if all lines all lit-up at once. He is struggling to respond timely with the skeleton crew staffing the Mega Co call center due to the extended holiday weekend. The team is reporting to Jose that they are getting a large number of irate callers complaining about charges to their Mega Co accounts.

# Monday Facts

He is doing the best he can; he is fighting a losing battle. Wait times are climbing and the calls just keep coming. He has never seen anything like this. He grabs a head set and punches up a few calls to try to understand what is happening. He hears callers complain about charges to their accounts, charges they did not make. They want action. Jose is looking for help and calls IT Security to see if they can help figure out what is happening. No one else is called.

# Monday Facts

Gerald, IT Information  Security Team member, receives a call from Jose, the manager of the Mega Co benefits help line call center.  Jose is looking for help in understanding why there is a sudden surge in calls.  Gerald asks for a download of the callers' information to see what he can find.  The one thing they all seem to have in common, they are Mega Co employees who transacted business with Benefits in the last quarter.

# Monday Facts

As he is beginning to work through the data received from Jose, Gerald receives a call from Maggie. The call is about a VP's lost tablet. As much as he would like to continue working the call center issues, he notifies his supervisor, Jane, who takes on the task of attempting to find an explanation for the call center activity. Gerald begins working the missing tablet issue.

# Monday Facts

Jane, IT Information Security Team supervisor, receives a call from Gerald asking for help. She is now working to see what, if anything, she can learn from the call center information forwarded by Jose. After some initial work, she is able to determine the information is similar to that found in the quarterly benefits reports issued by the company and used by HR.

# Monday Facts

Jane believes there is something not right and she calls the CPO [YOU] to discuss her findings and ask about next steps.

# Tuesday

# Tuesday Facts

Jane receives a call from Bruno, the VP of HR, looking for an explanation. At least four senior executives are calling him to complain about the charges to their accounts. Bruno tells Jane he was questioned about how HR could cause such a screw-up. Bruno wants to know why IT caused him so much grief. He is absolutely certain it has something to do with the e-commerce website. Jane tells Bruno he may want to talk to the CPO [you].

# Tuesday Facts

The CPO's [your] smart phone has not stopped ringing. The VP HR called. The CIO called. The four executives whose account information was wrong called. Jane from IT security called. Victoria called. In addition to the calls from internal people there is a call or two from local TV news stations. During one call the reporter says they are receiving calls from angry employees and a few of Mega Co's customers complaining about mysterious charges to their accounts.

# Wednesday

# Questions for the CPO

Everyone is looking to the CPO [you] to help sort out this mess.

- What do you do?
- What do you need to know?
- Whom do you ask?
- Is your resume up to date?

# Questions to Ponder

- Do you have an established incident response plan?
- Have you designated team members and assigned roles and responsibilities?
- If so, does your team meet regularly?
- Do you have a small core team for initial assessment?
- Is there a designated decision maker?
- Do you know who to call for help?
- Do you have outside forensic investigators, privacy counsel, and public relations experts lined up and ready to respond when you call?
- Do you plan to engage the outside experts from the start of an incident?
- Do you follow the privacy security events reported in the news, actions taken by regulators, and suits brought (and won or settled) by lawyers and learn from the mistakes and misfortunes of others?

PAI

# Questions to Ponder

- Have you practiced with your team?
- Do you know where all your organization's sensitive data is?
- Can you identify the applications and locations where the sensitive data resides?
- Do you have IT information sufficient to enable you to know which applications exist and who is authorized to access them on an ongoing basis?
- Are you limited to the US?
- If you are international, have you considered the privacy implications of your global operations and trans-border data flows?
- Do you know what they are?
- Do you have network logging enabled?
- Do you have anything in the log files?

# Questions to Ponder

- Are data backup processes, procedures, and practices well understood and managed?
- Do you have an effective data records management processes, including appropriate data classification, retention, destruction and litigation hold processes?
- Do you encrypt mobile devices and mobile storage devices?
- Are your security measures up to date and consistent with current best practices?
- Have you deployed and use data leak protection or similar technologies to provide insight to data movement?
- Do you have a process to effectively manage an investigation?
- Have you assessed risk from both external and *internal* threats?
- Are your vendor/supplier contracts drafted to require appropriate data practices from those with whom you share data?

PAI

# Questions to Ponder

- Has your organization established contacts with local law enforcement agencies?
- Do you know when to seek assistance from law enforcement?
- Is your team and process geared to react immediately?
- Does senior management have the necessary patience gain the facts before making public statements?
- Are you prepared to “stop the bleeding” and begin remediation as soon as practicable?
- Are processes in place to record and document your actions and why they were or were not taken?
- Do you document what facts the company knew and when?
- Do you have a process to meet with and regularly update the investigative team?

PAI

# Questions to Ponder

- Are you certain you are willing to wait for real numbers before issuing statements using preliminary and unsubstantiated numbers?
- Do you appropriately consider the impact to the business and risks associated with new findings?
- Will bad news really get better with age?
- Does the IT staff know what actions to take in response to an event?
- Have you weighed the consequences of shutting down the affected servers in the middle of an incident?
- Are you prepared to image the necessary servers and laptops from the beginning of an incident?
- Are you prepared to pull network logs immediately to preserve critical evidence and to increase log capacity as needed?

PAI

# Questions to Ponder

- Are you ready to take live memory dumps?
- Is there a plan to reset passwords quickly to reduce potential further comprise?
- Is your existing governance structure adequate and appropriate to respond in the event of an incident?
- Have you prepared your employee base with consistent messaging so they recognize the signs of a possible breach and know what to do and who to contact to report concerns?
- Is there a mechanism designed and operationalized to receive and react to reports of suspected incidents?
- Have you prepared and delivered effective and meaningful privacy and data security training to your employees?
- Have you consider how to engage your experts while also maximizing the protections afforded under the doctrine of legal privilege?

# Questions to Ponder

- Is your plan and process sufficiently sophisticated to capture, document and learn from an incident?
- Do you document and report incidents to management on a regular periodic basis?
- Will you be able to leverage an incident to obtain added funding for security?
- Have you prepared for a post incident follow-on regulatory inquiry?
- Are you putting the learning to good use through the use of privacy by design and privacy and security risk assessments when engaging with new initiatives?
- Do you have a comprehensive, implementable remediation plan including enhanced technology and security programs and the practice of data minimization and reduction efforts?
- Are you certain your remediation process will work?
- Has it been tested?

PAI

# Questions to Ponder

- Who pays for what?
- Who decides what is provided to effected data subjects to retain their goodwill?
- How do you determine if an incident is a notifiable breach?
- How do you determine notification obligations and who decides?

# Resources

Data Breach Notification - A Guide to Handling Personal Information Security Breaches - The Office of the Australian Information Commissioner
http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html

Privacy & Data Loss  Incident Readiness Planning Guide –Online Trust Alliance
https://otalliance.org/resources/incident/2012DataBreachGuide.pdf

Recommended Practices on Notice of Security Breach Involving Personal Information - California Office of Privacy Protection
http://www.privacy.ca.gov/business/recom_breach_prac.pdf

Dealing with a data breach – Federal Trade Commission
http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

Information Security and Security Breach Notification Guidance – Illinois Attorney General
http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf

PAI

# Contact Information

Keith Cheresko, Principal

Privacy Associates International LLC

40777 Lenox Park Drive, Suite 100

Novi, Michigan 48377

248.535.2819

kcheresko@privassoc.com

www.privassoc.com