



**PAI**

**PRIVACY ASSOCIATES INTERNATIONAL LLC**

---

# **Data Privacy Security Breach Exercise**

*ISSA Meeting*

*January 21, 2016*

# Purpose

- Provide a forum to discuss privacy security data incident/event issues
- Discuss how best to respond in the event of a privacy incident and learn from the experience of others in a safe, no risk environment
- Provide information for use in assessing existing breach response plans and adopt enhancements from the session learning.

# Methodology

- Create a factual scenario loosely based on past reported privacy incidents
- Ask participants to role play in delivering key facts
- Ask for comments from all as we proceed

# Terminology

“A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information.”

# Managing Data Breach Risk

- Understand legal obligations
- Consider technological protections
- Know your partners
- Educate staff
- Designate data security responsibility
- Have a data breach response plan

# Background

# MEGA CO

# “Congratulations, you’re hired”

Recently you accepted the Chief Privacy Officer position at Mega Co., a well respected Canada-based conglomerate. You are excited about the opportunity and can hardly believe you will get to put into practice all the wonderful things you have learned from participating in the local IAPP KnowledgeNet group and from attending IAPP conferences.



# Mega Co

Mega Co has retail and wholesale operations throughout Canada and the U.S. and is considering further international expansion. The company maintains active and successful e-commerce sites where customers may purchase products using its own 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 convert some of its in-house applications to similar applications available in the “cloud” to save money.

# Mega Co - Continued

Mega Co has several policies regarding acceptable use of social media and other electronic communications tools. However, it continues to adhere to a policy prohibiting employees from using their own mobile devices for company business despite a rather vocal desire by its employees to do so. 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

Mega Co. makes available to its employees a generous benefits package including a credit card program and health insurance plan administered through its centralized human resources department.



# Mega Co - Continued

Today is Friday, the day before a long holiday weekend and your added extra few days of a well deserved vacation. A number of your colleagues have already departed for points unknown and the office is feeling a little deserted, which is perfectly fine with you because you are looking forward to a nice, quiet long time off at the lake.

# Ready to Begin?

Wednesday



# Wednesday Facts

Victoria, VP - facilities development, is boarding a plane to return to Canada 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's team play in the local school's baseball tournament 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 worse 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. Imagine 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 place their coats on their 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 message 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 has 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 co-workers. Susan answers a call from Victoria. She hears the same stories over and over, somebody (this time a mucky-muck) loses their 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, Susan dutifully completes a lost device report form on *paper* and puts it in the “out” box. It’s late and she’s 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 Tuesday 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 can use to get ahead in 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 these types 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 plans to enjoy the upcoming week with extra money she now has to spend.



Monday



# Monday Facts

It's the holiday and everyone seems to be enjoying the day off. No one really seems to be concerned about work.

Tuesday



# Tuesday 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 about the lost flash drive, besides if he reports the loss he could be subject to disciplinary action.

# Tuesday Facts

Susan starts her day with a slight tinge of guilt. On her way to work today she heard a radio report about ID theft resulting from stolen and lost devices. She started wondering if she was right in submitting the report from Victoria on paper instead on the usual electronic form.

# Tuesday Facts

To put her mind at rest and soothe her slightly guilty feelings, Susan pulls the report (which was still sitting in the outgoing 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.

# Tuesday 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.

# Tuesday 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 really important. Having completed the information transfer, Maggie hangs up the phone and gets on with her day.



# Tuesday 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 meet SLA requirements to respond timely with just 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.

# Tuesday Facts

Jose 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 Mega Co. 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.

# Tuesday Facts

Gerald, IT Information Security Team member, receives a call from Jose, the manager of the Mega Co 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. Gerald uses his admin access to check a couple data bases he normally does not access. He discovers by cross referencing the data from several sources the one thing the callers all seem to have in common, they are Mega Co employees who transacted business with Benefits in the last quarter.

# Tuesday 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.

# Tuesday 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.

# Tuesday Facts

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

Wednesday



# Wednesday 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].



# Wednesday 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.

# Thursday



a/k/a

“The day the fecal matter hits the  
oscillating blades”

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?

Thoughts? Questions?



# Contact Information

Keith Cheresko, Principal  
Privacy Associates International LLC  
40777 Lenox Park Drive, Suite 100  
Novi, Michigan 48377  
248.535.2819  
[kcheresko@privassoc.com](mailto:kcheresko@privassoc.com)  
[www.privassoc.com](http://www.privassoc.com)

