# WORKSHOP PREPARATION (FOR AT1 & AT2)

## INFO30006: INFORMATION SECURITY AND PPRIVACY

**Week 04 - Workshop 03: 16 and 17 August 2017**

*Workshop facilitator: Dr Jeb Webb*

**WORKSHOP WEEK 04: MANAGING SECURITY RISKS**

**Due date:** Weekly at workshops during Week 03 to Week 12.

**Weight:** **Assessment task 1**: **20%**

- **Assessment task 1a:** group presentation in workshop (10%)
- **Assessment task 1b:** group facilitation of workshop discussion (105)

**Assessment task 2: 10%**

- Individual participation in workshop by all (10%)

**Workshop format:** Workshops are 1 (ONE) hour. The following proposed planning of workshop time should be respected by presenting group, as workshop will subsequently be managed by facilitating group.

| **~ 60 minutes:** | **Workshop:** |
|---|---|
| 5 minutes: | Sign attendance sheet/get ready for the session |
| 15-20 minutes: | Presentation of material by one group: *group x* |
| 30-35 minutes: | A second group, *group y*, facilitates workshop discussion based on presentation |
| 5 minutes: | Final questions and answers (Q&A) |

## YOUR TASK - ALL:

### PREPARATION OF TOPIC-RELATED MATERIAL:

This week, we discussed risk management by building on concepts from last week, i.e., asset, threat, vulnerability, and risk. We clarified, there is a difference between the three concepts and how they relate to each other. We looked at different security threats and security risks in society, today as well as in the near future, before considering the risk management process. The process of managing security risks is fairly simple in theory; yet very cumbersome in practice. Most often risks are assessed without access to an adequate level of information – however, there is still a justification for investing in effective information security risk management processes to:

1. ensure the correct identification of information assets and risks
2. select and implement the most effective control strategies

This week's workshop relates to the security, threats, and risks, organisations face as information security threats are having more severe consequences than ever before. One such organisation is the Australian Red Cross' (ARC) Blood Service 'DonateBlood'…

On 5 September 2016, a file containing information relating to 550,000 blood donors and their personal details (1.28 million records) was saved to a public-facing web server administered by a third party provider. A data breach occurred and an unauthorised individual accessed the data on 25 October 2016.

On 27 October 2016, the Australian Information and Privacy Commissioner, Timothy Pilgrim, opened an investigation into the incident under the *Privacy Act 1988* (Cth) based on the large number people who could potentially be affected as well as the sensitivity of the data (including sexual and medical histories). The Commissioner also opened a separate investigation into the information handling practices of the third party provider.

This Commissioner concluded the investigation on Monday 7 August 2017, and the investigative reports of the Australian Red Cross' Blood Service and the third party provider, who administered the web server, Precedent Communications Pty Ltd, have been released.

**Workshop task**:

1. Read the two investigation reports and other referenced material attached, mainly:
   - 1.1 'DonateBlood.com.au data breach (Australian Red Cross Blood Service)'
   - 1.2 'DonateBlood.com.au data breach (Precedent Communications Pty Ltd)'

2 Prepare answers for each of the following questions

- 2.1 In the above case, the data breach was caused by human error, however, the reports mention certain measures the Blood Service and the third part provider could have taken to mitigate or maybe even avoid the data breach. What were they? And do you think these measures could have prevented the breach?
- 2.2 The main cause of the data breach is cited as being 'human error'. Apart from storing a data file on a public-facing web server, consider other types of human error that could cause an incident and reflect upon whether it is possible to protect assets from human errors.
- 2.3 Are organisations who outsource (some of) their information security function to protect their assets taking further or fewer risks than organisations with their own information security function? Justify your answer.

3 Concluding remarks

**Added documents on LMS:**

Australian Government: Office of the Australian Information and Privacy Commissioner, 2017, 'DonateBlood.com.au data breach (Australian Red Cross Blood Service)', 7 August 2017: https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-australian-red-cross-blood-service.pdf

Australian Government: Office of the Australian Information and Privacy Commissioner, 2017, 'DonateBlood.com.au data breach (Precedent Communications Pty Ltd)', 7 August 2017:

https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/donateblood-com-au-data-breach-precedent-communications-pty-ltd.pdf

McIlroy, T, Hunter, F, Spooner, R, 2016, ‘Red Cross data leak: personal data of 550,000 blood donors made public’, Sydney Morning Herald, 28 October 2016: http://www.smh.com.au/federal-politics/political-news/red-cross-data-leak-personal-data-of-550000-blood-donors-made-public-20161028-gscwms.html

Spencer, L, 2017, ‘Red Cross Blood Service partner owns up to data breach blunder’, *CIO Magazine*, 7 August 2017: https://www.cio.com.au/article/print/625715/red-cross-blood-service-partner-owns-up-data-breach-blunder