An Effective Approach for Dealing with the Pressure to Compromise Security During Systems Development

Yeslam Al-Saggaf(✉)

School of Computing and Mathematics, Charles Sturt University,
Boorooma Street, Wagga Wagga, NSW 2678, Australia
yalsaggaf@csu.edu.au.com

Abstract. This study looks into (1) the frequency with which Australian IT professionals compromise security to meet deadlines; (2) the causes of unprofessional behavior in the IT work place; (3) the best approach for tackling unprofessional behavior; and the effectiveness of this approach. These issues were addressed using a mixed research methodology that involved three data collection stages with the input of each stage being the output of the earlier stage. In the first stage, we conducted a survey of 2,315 Australian IT professionals which the Australian Computer Society helped promote. In the second stage, we interviewed 43 Australian IT professionals from six different Australian state capitals to understand the causes of unprofessional behavior in the IT work place and the best approach for tackling unprofessional behavior. Following the research participants' suggestions, I implemented the approach suggested by the majority of participants. I then shared the links of the approach I implemented with the Australian IT professionals via the Australian Computer Society. In the final stage, I interviewed 28 IT professionals to receive their feedback with regards to the effectiveness of this approach in enhancing young IT professionals' abilities to recognize unprofessional behavior. This paper presents the results from the three stages of this study.

Keywords: Compromising security · Australian organizations
Systems development · IT professionals · Professional ethics

1 Introduction

The aim of this paper is to report findings relating to the commonness of compromising security from the viewpoint of Australian IT professionals from a study that investigated unprofessional behavior in the IT work place in Australia more generally. Another aim of this paper is to investigate the causes of unprofessional behavior more generally. Third, to discover the best approach for tackling unprofessional behavior. Fourth to evaluate the effectiveness of this approach.

The study, which is part of a larger project on professionalism in the IT work place, involved collecting data during three phases. In phase one, we conducted an online survey of 2,313 members of the Australian Computer Society (ACS), which we administered using SurveyMonkey. The data from this phase indicated that compromising security is

X. Lin et al. (Eds.): SecureComm 2017 Workshops, LNICST 239, pp. 32–46, 2018.
https://doi.org/10.1007/978-3-319-78816-6_3

one of the top ten unprofessional behaviors that IT professionals commit in the IT work place (Table 2 lists the top ten unprofessional behaviors). In the next step of data analysis, we looked at the characteristics of the survey participants who selected compromising security as one of the unprofessional behaviors. This information is important for understanding the profile of the IT professionals who identified compromising security during systems development as a problem. In phase two we conducted qualitative interviews with 43 IT professionals. We selected the IT professionals we interviewed from the survey participants who indicated their willingness to participate in this phase when completing the survey. The face-to-face conversations with the IT professionals offered valuable clues into the causes of the unprofessional behavior in the IT work place in general and the best approach for tackling unprofessional behavior. In accordance with the interviewees' suggestions, I implemented the approach suggested by the greatest number of participants. I implemented the approach suggested by the majority of participants. I then shared the links of the approach I implemented with the Australian IT professionals via the Australian Computer Society. In the final stage, I interviewed 28 IT professionals to receive their feedback with regards to the effectiveness of this approach in enhancing young IT professionals' abilities to recognize unprofessional behavior.

The paper begins by introducing the research questions. Next, the research methodology and the findings from the quantitative survey are presented. The process of collecting data using semi-structured interviews is discussed next, followed by a discussion of the findings from this qualitative component of the research relating to the causes of unprofessional behavior in general and the most effective approach for tackling unprofessional behavior in the IT work place. This is followed by a discussion of the feedback about the implemented approach. The paper ends with a comparison of the findings from both approaches.

2 Background

Cybercrime costs the Australian economy more than AU$4.5 billion annually [1]. The Australian Crime Commission laments the loss of this money that they say could otherwise be used to fund services, roads, hospitals and schools in Australia [2]. The 2016 Australian Cyber Security Centre Survey found that 90% of the Australian organizations surveyed experienced a cyber security breach or threat during the 2015-16 financial year that compromised the confidentiality, integrity or availability of network data or systems [3]. The above statistics for Australia are consistent with international trends. Juniper Research predicts the cost of security breaches to reach $2.1 trillion globally by 2019 [4]. At the individuals level, more than 46,957, cybercrime incidents have been reported to the Australian Cybercrime Online Reporting Network (ACORN) in 2016 up from 39,491 in 2015 [5]. Between 1 January 2017 and 31 March 2017, 11,775 incidents were reported to ACORN up from 9,679 during the same period in 2015 [5] suggesting that cybercrime incidents are on the rise.

As cyber-criminals and hackers continue to discover and exploit vulnerabilities in information systems, the need for securing information systems has never been greater. The above statistics and Lucas and Weckert [6] study findings that suggested that

compromising security to meet deadlines or make things work is a problem facing IT professionals, raise the following question:

RQ1: How often is security compromised to meet deadlines?

There are several reasons behind unprofessional behavior in the IT work place more generally and compromising security during the development of information systems more specifically. One reason could be IT professionals' lack of awareness when it comes to recognising ethical problems in the work place or providing solutions to them especially when two or more priorities are at tension with each other (i.e. the interest of the employer versus the interest of the client etc.) [7, 8]. A study by Lucas and Weckert [6], for example, found that "ethical awareness in the IT profession requires some strengthening" (p. 42) and that "IT professionals do not have a conscious awareness of the ethical notions that are most important in their work" (p. 47). There is evidence that suggests that ethics awareness has led to a higher level of professionalism and ethical behavior among IT employees (see Al-Saggaf and Burmeister [9], Cappel and Windsor [10], and Van den Bergh and Deschoolmeester [11]). Higher levels of professionalism resulted in improvement in the performance of the IT industry and the quality and delivery of IT products and services [12]. This has led scholars to argue for the need to raise awareness of ethical issues among IT professionals [12]. Another reason is IT professionals' selfishness. Cappel and Windsor [10] argue that IT professionals may be tempted to view ethical issues from an egocentric point of view, thereby either over-simplify situations or fail to consider alternatives, stakeholders, consequences, or one's duties. A third reason is pressure. While the IT industry tries to address its shortcomings through the use of rigorous software and application development methodologies, quality assurance initiatives, risk management approaches, and external assessment processes, these largely tend to get ignored when management and personnel are under pressure to perform (see [6, 13, 14]). Lucas and Bowern [15] note that pressure to complete projects on time can make IT professionals compromise ethical standards and policies or even break the law. The second research question is therefore:

RQ2: What are the reasons behind unprofessional behavior in the IT work place?

While many studies focused on ethical decision-making (see, for example, Anderson et al. [16], Al-Saggaf and Burmeister [9], and Fleischmann [17]), few studies focused on how IT professionals actually recognize and solve ethical problems in their workplaces (see Lucas and Bowern [15], and Khanifar et al. [18]). Lucas and Mason [13] conducted a study to determine the ethical attitudes of Australian IT professionals, however, they did not focus on how these professionals identify problems or employ strategies to resolve the ethical dilemmas they face in their day to day work. That said, with the exception of Nielsen [19] and Jamil and Susanto [20], who proposed changing organisational culture as a approach to avoid unprofessional behavior, most of the studies that offered recommendations relating to how to identify and resolve ethical problems were for use by students in the classroom. These include using codes of ethics (see Anderson [16], Burmeister and Weckert [21], and Gotterbarn, [22]); case studies and scenarios (see Ferguson et al. [23] and Maslin et al. [24]); the use of role play (see Johnson [25] and Fleischmann, [17]); the doing ethics technique

(see Seach et al. [26]); and critical thinking and argument mapping using Rationale (see Al-Saggaf and Burmeister [9]). The third and fourth research questions are therefore:

RQ3: What is the best approach for tackling unprofessional behavior in the IT work place?
RQ4: How effective is this approach?

3 Methodology and Results

3.1 Stage 1: Survey

Survey Procedure. The first stage of the data collection comprised administering a survey via SurveyMonkey so respondents can complete it electronically. The survey design was informed by the design of Lucas and Weckert's [6] survey study which they conducted in 2006 survey. We invited all recipients of the ACS Information Age to complete the questionnaire by a direct email sent to them by the ACS in 2013. The survey was closed within less than two months when the response rate reached 12.4%. We prefaced the online survey by an ethics information statement which included a description of the study. Questions were both closed and open-ended. This paper reports on only the closed questions.

Sample. 2,315 respondents filled the questionnaire. The average number of years of work experience for the participants was 19 years; however, the average number of years of work experience for the respondents who selected compromising security as one of the common unprofessional behaviors was 20.3 years. Table 1 shows a summary of the demographic information for the respondents overall as well as for those who identified compromising security as one of the common unprofessional behaviors. As can be seen from Table 1, the overall profile of the survey participants is similar to the profile of those who selected compromising security as one of the one of the common unprofessional behaviors.

The Commonness of Compromising Security in the Australian IT Work Place. We asked respondents to the survey to select from among different unprofessional behaviors that they witnessed in their work places. Given we allowed respondents to select more than one answer, we judged multiple response frequency analysis to be suitable for analyzing this question. We also performed cross tabulations to find out if there were variations in answers based on the characteristics of participants. The results from the multiple response frequency analysis and the cross tabulations are shown below.

The multiple response frequency analysis shown that compromising security was ranked tenth in a list of the most common unprofessional behaviors witnessed by IT professionals (n = 611, 26.4%). Table 2 shows the top 10 unprofessional behaviors along with the number of responses and their proportions. This paper focusses on compromising security; thus discussions of other unprofessional behaviors listed in Table 2 are outside the scope of this paper.

Table 1. Demographic characteristics of the survey participants and those who selected compromising security as an ethical issue in the survey.

Demographic information		Survey participants		Participants who selected compromising security	
		N	%	N	%
Gender	Female	356	15.5	84	13.7
	Male	1,940	83.9	524	85.8
	N/A	17	0.7	3	0.5
Age	<35	692	30	166	27.1
	36–45	516	22.3	161	26.4
	46–55	576	25	157	25.7
	>56	524	22.7	126	20.6
	N/A	5	0.2	1	0.2
State	ACT	247	10	72	11.8
	NSW	696	30.4	170	27.8
	NT	27	1.2	6	1
	QLD	279	12.2	71	11.6
	SA	120	5.5	39	6.4
	TAS	42	1.8	16	2.6
	VIC	581	25.4	161	26.4
	WA	218	9.5	60	9.8
	Overseas	80	3.5	13	2.1
	N/A	23	1.0	3	0.5
Occupation	Administrator	134	6.5	49	8
	Consultant	502	24.3	153	25
	Developer	307	14.8	83	13.6
	Education	150	7.3	27	4.4
	Manager	698	33.8	182	29.8
	Technical Support	277	13.3	64	10.5
	Other	215	10.39	51	8.3
	N/A	247	11.9	2	0.3
Geographical location	Capital city	2,069	89.5	550	90.0
	Regional area	215	9.43	57	9.3
	N/A	29	1.3	4	0.7
Job classification	Business owner with employed staff	57	2.7	13	2.1
	Fixed term contractors	251	11.8	76	12.4
	Indefinite contractors	34	1.6	13	2.1
	Permanent full-time	1,388	65.4	406	66.4
	Permanent part-time	90	4.2	18	2.9
	Self-employed	112	5.3	31	5.1
	Temporary full-time	61	2.9	15	2.5
	Temporary part-time	63	3.0	8	1.3
	Volunteer	67	3.2	10	1.6
	Other	121	5.69	19	3.1
	N/A			2	0.3

Table 2. The top 10 unprofessional behaviors witnessed by Australian IT professionals

Ethical problems	Number of survey respondents	
	N	(%)
Compromising quality	1104	47.7
Blaming others for own mistakes	957	41.4
Compromising functionality	846	36.6
Overworking staff	762	32.9
Incompetence	750	32.4
Conflict of interest	682	29.5
Unprofessional behavior	633	27.4
Compromising user requirements	632	27.3
Bullying	630	27.2
Compromising security	611	26.4

We wanted to find out which participants characteristics predict participants' choice of compromising security in the survey. To answer this question, we used generalized linear models (GLMs). The responses to the compromising security question are dichotomous (recorded as a Yes/No), whereas all the demographic variables are categorical. To investigate the relationships between the predictor variables and the dichotomous response variable, we fitted GLMs. We carried out the GLMs using *R* (version 3.0.2). We verified all requirements of this analysis were.

The analysis of deviance shown a significant relationship between participants' selection of compromising security as an unprofessional behavior in the survey and occupation and job classification (see Table 3). No other demographic variables showed evidence of a relationship.

Table 3. The analysis of deviance

Demographic variable	Deviance	Degrees of freedom (DF)	P
Occupation	18.38	6	0.0053
Job classification	32.32	11	0.0007

We also used GLMs to investigate if there is a relationship between the prevalence of unethical conduct and the participants' choice of compromising security. We fitted this technique to examine this relationship since the predictor is also a categorical variable. The analysis of deviance revealed a significant relationship between the prevalence of unethical conduct and participants' choice of compromising security ($Deviance = 91.23$, $df = 4$, $p = 0.00$) suggesting this variable is likewise a predictor for participants' selection of compromising security.

The analysis of deviance also revealed that occupation predicted the choice of compromising security. Twenty-five percent of the participants who selected compromising security as a frequent unprofessional behavior were consultants and 29.8% were managers. In contrast, only 13.6% of the respondents who selected compromising security as an unprofessional conduct were developers. This shows that participants in senior positions are more worried about compromising security than participants in non-senior positions Likewise, we also found job classification to be a predictor of the choice of compromising security. A greater percentage of permanent full time employees (66.4%) and fixed term contractors (12.4%) selected this issue in the questionnaire. The full time permanent employees group is not surprising, but the fact that a large percentage of fixed term contractors selected this problem indicates that fixed term contractors are particularly worried about this issue. A future research study could provide insights with regards to the reasons for this surprising finding.

3.2 Stage 2 and 3: Qualitative Interviews

Conducting the Interviews and Analysing the Data. The survey stage was followed by two stages of semi-structured interviews (43 participants in the second stage and 28 participants in the third stage). Participants were all selected from the respondents of survey who indicated willingness to participate in the future stages of the project. We conducted the second stage interviews in 2014 and the third stage interviews in 2017. We conducted sixty-six interviews (43 interviews in the second stage and 23 interviews in the third stage) were face-to-face and took place in the six Australian state capitals. We conducted the remaining five interviews (third stage) via Skype. We audio recorded and transcribed verbatim all interviews.

We sent the invitation for participation to all survey respondents who indicated that they were willing to take part in interviews during the project's stage one. We selected the interviewees based on their characteristics and ensure that a diverse range of backgrounds were represented. The final list of participants included IT professionals from a diverse range of organizations, such as large and small and who come from all Australian state capitals and represent different ages, genders, kinds of jobs, and work experiences. Table 4 lists the characteristics of these individuals.

We analyzed the transcribed interviews using qualitative thematic analysis with the help of NVivo. We used each transcribed interview document as the unit of analysis. We performed data analysis as follows. (1) We read the interview documents several times. (2) We created nodes based on keywords and dominant phrases in the transcribed documents. (3) We located text within the interview documents with the same nodes and assigned it to these nodes. This way each node acted as a "bucket" in the sense that it held all the data related to a specific node. These nodes were then further divided into specific sub-nodes. This was done to create a hierarchy so it is easier to interpret the findings.

Table 4. Characteristics of the interviewees

Interviewees' characteristics		N
Gender	Female	12
	Male	59
Age	<35	5
	36–45	10
	46–55	26
	>56	26
Occupation	Accreditor	1
	Business analyst	5
	Consultant	12
	Database developer/coordinator	2
	Manager	19
	IT educator	4
	Retired	6
	Other	22
City	Adelaide	9
	Brisbane	8
	Canberra	8
	Melbourne	12
	Sydney	17
	Perth	12
	Skype	5
Job classification	Fixed term contractors	19
	Permanent full-time	52
IT work experience (years)	10–19	9
	20–29	15
	30–39	24
	>40	23

The Causes of Unprofessional Behavior. While the findings from the 43 interviews revealed 25 reasons behind unprofessional behavior in the IT work place only the reasons brought up during interviews by the highest number of interviewees, in this case 18 out of the 43, will be discussed below. Two reasons met this condition: bad management and pressure. Other reasons include greed, lack of respect for IT people, poor communication skills, self-interest, IT project's complexity, fear of losing job and lack of awareness, to name a few. These findings are consistent with the literature pertaining to the main reasons behind unprofessional behavior in the IT work place (see Background section above) specifically with regards to lack of awareness, self-interest and pressure.

Eighteen out of 43 participants identified bad management as one of the causes of unprofessional behavior in the IT work place. The following quote typifies their views:

> What leads to unprofessional behavior therefore is probably a poor management structure and a set of values that aren't clearly defined or at least not communicated yeah.

The 18 interviewees who raised bad management during interviews expressed a range of views about this issue including the view that when management engages in unprofessional behavior, unprofessional behavior trickles down to staff:

> I have seen where a team leader or a manager perhaps behaves in a certain way, you'll see that behavior reflected through his organization and that's not necessarily helpful.

One interviewee agreed maintaining that ethical behavior has *"got to come from management down"*, a view which a third interviewee also shared:

> it gets driven from the top. So if you've got a leader who, so a Chief Executive who acts like that, who then, the directors follow that because he's acting in that way, they all follow in that same way. Then you have the managers who also act because the CEO's demonstrates in a behavior, the directors are, the managers are, and then because the manager is the staff also believe that that's the way.

Both of the above quotes emphasise the importance of *"leading by example"* in reducing unprofessional behavior in the IT work place.

Similarly, 18 out of 43 participants identified pressure as one of the causes of unprofessional behavior in the IT work place. The 18 interviewees who raised this issue during interviews reported several examples of pressure facing IT professionals. There is pressure on project managers to provide inaccurate estimations of costs of projects:

> And there's always a pressure on there, well if I, if I made an estimate based on what I actually think it's going to take, how much … it going to take me cost, I probably wouldn't succeed. So there's, some pressure either to make it seem smaller than it really is in order to get any money at all or the other one which says I applied some weird factor.

There is pressure on salesmen to sell unwanted products and services because they are paid leveraged salaries:

> when you're sitting on a leveraged salary that's 5545 somewhere along the line something's got to give and if you're not having a good quarter, the following quarter you've got to have a good quarter otherwise you won't keep the kids. So it's a dilemma and more and more organizations are heading towards leverage state and that drives the sales behavior.

There is pressure on program managers to cut corners to secure the next contract:

> Early delivery thing where you're getting pressure from the people above to do something and the thing wasn't the pressure to do something quicker because we're doing that all the time. As a program manager you've got all these things to sort of hit but when it's the reason for doing it is because then they might get another contract, to me that was the ethical question.

It clear from the above examples that financial gain underpins all these pressures.

The Best Approach for Tackling Unprofessional Behavior. While the findings from the 43 interviews revealed 21 approaches for tackling unprofessional behavior in the IT work place only the approaches brought up during interviews by the highest number of interviewees, in this case 26 out of the 43, will be highlighted below. One approach met this condition: case studies. 26 out of 43 participants suggested the use of case studies as an effective approach for tackling unprofessional behavior in the IT work place. The literature has also identified case studies as an effective approach for tackling unprofessional behavior in the IT work place (see Background section above). Other

approaches suggested include a mentoring program for young IT professionals and a 'helpline' through which young IT professionals can receive counselling.

One reason the highest number of interviewees suggested the use of case studies is because case studies can enable IT professionals to *"be in someone else's shoes"* as one interviewee argued *"Putting yourself in the shoes of one of those other stakeholders is a key."* Case studies can enable IT professionals to ask themselves: what would I do in such a situation?:

> Every now and again there's an article in the Information Age which has case studies, I enjoy case studies…. I always read them and think "Oh yeah, what would I do?"

Case studies can enable IT professionals to learn from other people's mistakes: *"In IT one can learn very well by example"* because, according to this interviewee *"we study what's come before."* But one interviewee warned:

> Scenarios shouldn't be black and white… You should know when you're in the dark grey area cause that's the problem area, that's the stuff that we need to fix.

Black and white scenarios are straightforward and thus they are not helpful. They need to be grey so individuals can relate them to their circumstances: *"I'm likely to go in on the test cases looking for the closest of what's happening to me."*

Case studies can enable IT professionals to consider a situation from multiple perspectives:

> If you can provide somebody in a situation where they're trying to make a decision, both perspectives, you'll do, like that would be really valuable.

Case studies can also enable IT professionals to consider the risks*: "we're trying to give them an understanding of some of the risks that are out there. Some real examples."* Other interviewees also shared this interviewee's suggestion regarding the use of real examples because, as another interviewee explained, *"People relate to real scenarios."*

The Effectiveness of the Implemented Approach: Interactive YouTube Videos. In response to the interviewees' recommendation regarding the use of case studies as an effective approach for tackling unprofessional behavior in the IT work place, we developed four interactive YouTube videos highlighting cases of unprofessional practice. One of the videos specifically addresses the conduct of compromising security due to pressure from above. The video, which is titled "Early Launch", shows a situation in which a project manager is put under pressure to compromise the security of a system along with three short action videos that highlight the options to tackle the behavior and the potential outcome of each option. These videos enable IT professionals to choose options and then see the outcome of their selections. The objective of the three action videos is to enable the IT professionals watching the video to question themselves what they would do in such a scenario by selecting an action for tackling the behavior and then see the outcome of that action.

Following the development of the videos, we uploaded these videos on the ACS YouTube Channel. Next, we interviewed 28 IT professionals to provide feedback on the effectiveness of these videos in improving IT professionals' ability to recognize unethical conduct at work. The majority of interviewees agreed that these interactive

YouTube videos and their outcome videos are valuable to have. The following comments summarize their views:

- *I like the approach of the scenarios and that sort of thing*
- *Well I think sometimes role play is not bad which is what this video does*
- *I liked the examples that you had in your video*
- *Well I think sometimes role play is not bad which is what this video does*
- *Some aspects of the video were good*
- *At the higher level I think where the ethics really, within organizations, where the ethics really starts to be an issue and that's why I like in that last, the video on early, the early [launch]*
- *I think it's fantastic. I think it's a really good way to create an interactive resource, especially for a DE student. Because there's a lot of resources for face to face, there's classes, you can ask questions. But with these videos, anytime, anywhere, you can constantly review it*
- *I like the approach of the scenarios and that sort of thing*
- *Yeah, it's good. I think it's a good idea. People can – you know, that can trigger people's memories, you know, and they say, oh yeah, I'll come across with you. This is something that happened here, happened there, and it's good*
- *Yes. I thought the encryption one was good. You made a clear point. It probably hit a nerve because there's been so much problems recently with the ABS and those sort of things*
- *I thought the people in the videos were very believable*
- *But I think more often than not the rules aren't there so therefore they'll do like you said in the video, they'll respond at the time to what happens*
- *But what I thought was I thought the production qualities were excellent. I thought the acting was excellent*

Similarly, the following comments that these interviewees made about the approach of selecting possible actions then see the outcome of their selections typify their views:

- *I think that that's, that's what's attractive about it*
- *I liked it a lot, the, as I say, the only negative I have was the extreme anger in the two options-*
- *I think the training videos themselves, that ability to choose an action based on a set of circumstances I think is very important because that's what makes people pay attention to what's going on. If you just go and stick a video in front of them they're not going to take it is as much as something that's interactive;*
- *Yeah that was okay, what would you do in effect, or what – I think you were saying if you were in that position what would you do?*
- *I think they're – I mean I think they're good options*
- *I think it was good that they were able to see the outcomes*
- *Yeah I think that's excellent, that's what I think, but people – especially young people because they can't necessarily imagine that"*
- *It's good. Yeah, it's a good idea; Oh I actually – the way they played out was absolutely real world*

- *I think it's useful to get, to think through that there are consequences to decisions. There are consequences to people's lives, careers, products, projects, and just cutting code. There is much more to life and in IT and health IT than cutting code*

The above quotes shows that the interviewees thought the approach of selecting possible actions then see the outcome of their selections is effective. Further analysis will be conducted on the data from this final stage to find out how the videos can assist IT professionals with recognizing unethical conduct in the IT work place.

4 Discussion

The first research question addressed the prevalence of compromising security during system development within Australian organizations. The survey we conducted with a large sample of IT professionals showed that compromising security is one of the top ten unprofessional behaviors witnessed by Australian IT professionals in their work places. The analysis revealed a significant relationship between participants' choice of compromising security and occupation and job classification. Twenty-five percent of the respondents who identified compromising security as a frequent unprofessional behavior were consultants and 29.8% were managers. In contrast, only 13.6% of the respondents who selected compromising security as an unprofessional behavior were developers. This shows that respondents in senior positions are more worried about compromising security than respondents in non-senior positions. Interestingly 13.2% of the survey respondents who chose compromising security and 13.9% of the interviewees who brought up this issue in interviews classified their jobs as fixed term contractors. That fixed term contractors are more worried about compromising security than the permanent professionals is worthy of further investigation. Why these IT professionals ordered compromising security in the survey as a frequent unethical conduct and brought up this concern during interviews. Could it be because those external contractors are more worried about compromising security than the internal staff? Additional research is needed to shed light on this issue. It is hoped, this paper will inspire undertaking such an inquiry.

Qualitative interviews were conducted over two periods of time to address the second, third and fourth research questions. The second research question was concerned with the causes of unprofessional behavior in the IT work place. The qualitative analysis from the first round of qualitative interviews identified bad management and pressure as the top two in the list of the causes of unprofessional behavior in the IT work place. In terms of bad management, the qualitative analysis revealed that ethical behavior *"gets driven from the top"* and unprofessional behavior trickles down to staff. With regards to pressure, which the literature has also identified as a main reason for unprofessional behavior, the qualitative analysis revealed that financial gain underpinned all the kinds of pressures reported by the interviewees in this study. The third research question was concerned with the best approach for tackling unprofessional behavior in the IT work place. Twenty six out of 43 participants suggested the use of case studies as an effective approach for tackling unprofessional behavior in the IT work place. The literature has also identified case studies as an effective approach. Several reasons were highlighted for

why the highest number of interviewees suggested the use of case studies. The main reason however was because case studies can enable IT professionals to 'be in someone else's shoes.' Having implemented the suggested approach, the fourth research question was concerned with the effectiveness of the implemented approach (the interactive YouTube videos). The findings from the second round of qualitative interviews revealed that the majority of interviewees agreed that these interactive YouTube videos and their outcome videos are valuable to have and that enabling the viewers to make choices and then see how these choices play out is a good idea.

5 Conclusion

The aim of this study was to address the following research questions: how often is security compromised to meet deadlines? What are the causes of unprofessional behavior in the IT work place? What is an effective approach for tackling unprofessional conduct? To what extent this approach is effective? To fulfil the aims of the project we employed a mixed methodology comprising three stages of data gathering the input of each stage being the output of the earlier stage. The data collection proceeded as follows. In the first stage, we conducted a survey of 2,315 Australian IT professionals which the Australian Computer Society helped promote. The survey revealed that compromising security is one of the top ten most frequently witnessed unprofessional conducts. Based on the findings from this stage we rewrote the content of the follow-up interviews. In the second stage, we interviewed 43 Australian IT professionals from six different Australian state capitals to learn from them, the causes of unprofessional behavior in the IT work place and the best approach for tackling unprofessional behavior. The first round of qualitative interviews identified bad management and pressure as the top two in the list of the causes of unprofessional behavior in the IT work place. According to these interviews also, the highest number of interviewees suggested the use of case studies as an effective approach for tackling unprofessional behavior. In accordance with the interviewees' recommendations, I implemented the approach suggested by the majority of participants. I then shared the links of the approach I implemented with the Australian IT professionals via the Australian Computer Society. In the final stage, I interviewed 28 IT professionals to hear their comment with regards to the effectiveness of this approach in enhancing young IT professionals' abilities to recognize unprofessional behavior. The first impressions from the second round of qualitative interviews with regards to the effectiveness of this approach were all positive.

Acknowledgments. This project was supported by an Australian Research Council Linkage grant (LP130100808). The industry partner in this project was the Australian Computer Society. Professor John Weckert, A/Prof Oliver Burmeister and Mr John Ridge were the other team investigators. The author wishes to thank A/Prof Oliver Burmeister for his significant contribution to the project in general and specifically for helping with the distribution of the survey, conducting some of the qualitative interviews and his suggestions with regards to the analysis of the qualitative data. The author also wishes to thank Rachel MacCulloch (Charles Sturt University) for her suggestions.

References

1. Acumen Insurance Brokers. http://acumeninsurance.com.au/2017/03/14/cybercrime-costs-the-australian-economy-over-4-5-billion-annually-and-is-now-in-the-top-5-risks-faced-by-businesses/
2. Australian Crime Commission. https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/oca2015.pdf
3. Australian Cyber Security Centre. https://www.acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf
4. Juniper Research. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
5. Australian Cybercrime Online Reporting Network. https://www.acorn.gov.au/resources
6. Lucas, R., Weckert, J.: Regulation in the IT industry. Centre for Applied Philosophy and Public Ethics, Canberra (2008)
7. Sherratt, D., Rogerson, S., Fairweather, B.: The challenge of raising ethical awareness: a case-based aiding system for use by computing and IT students. Sci. Eng. Ethics **11**(2), 299–315 (2005)
8. Jung, I.: Ethical judgments and behaviors: applying a multidimensional ethics scale to measuring IT ethics of college students. Comput. Educ. **53**(3), 940–949 (2009)
9. Al-Saggaf, Y., Burmeister, O.K.: Improving skill development: an exploratory study comparing a philosophical and an applied ethical analysis technique. J. Comput. Sci. Educ. **22**(3), 1–19 (2012)
10. Cappel, J.J., Windsor, J.C.: A comparative investigation of ethical decision making: Information systems professionals versus students. Database Adv. Inf. Syst. **29**(2), 20–34 (1998)
11. Van den Bergh, J., Deschoolmeester, D.: Ethical decision making in IT: discussing the impact of an ethical code of conduct. Commun. IBIMA, 1–10 (2010)
12. McLaughlin, S., Sherry, M., Carcary, M., O'Brien, C.: e-Skills and IT Professionalism: Fostering the IT Profession in Europe. Final report. Maynooth, Innovation Value Institute, National University of Ireland (2012)
13. Lucas, R., Mason, N.: A survey of ethics and regulation within the IT industry in Australia: ethics education. J. Inf. Commun. Ethics Soc. **6**(4), 349–363 (2008)
14. Ethics Resource Center. http://www.ethics.org/ecihome/research/nbes/nbes-reports/nbes-2013
15. Lucas, R., Bowern, M.: Ethics survey: haste sours quality in IT. Information Age, June/July 2007, pp. 28–30 (2007)
16. Anderson, R.E., Johnson, D.G., Gotterbarn, D., Perrolle, J.: Using the new ACM code of ethics in decision making. Commun. ACM **36**(1), 98–107 (1993)
17. Fleischmann, K.R.: Preaching what we practice: teaching ethical decision-making to computer security professionals. In: Sion, R., Curtmola, R., Dietrich, S., Kiayias, A., Miret, J.M., Sako, K., Sebé, F. (eds.) FC 2010. LNCS, vol. 6054, pp. 197–202. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14992-4_18
18. Khanifar, H., Jandaghi, G., Bordbar, H.: The professional and applied ethics constituents of IT specialist and users. Eur. J. Soc. Sci. **27**(2–4), 546–552 (2012)
19. Nielsen, R.P.: Changing unprofessional organizational behavior. Acad. Manag. Exec. **3**(2), 123–130 (1989)
20. Jamil, N., Susanto, E.: Preventing unprofessional behavior of firms' managers through shame as a corporate culture. J. US-China Public Adm. **6**(7), 57–64 (2009)

21. Burmeister, O.K., Weckert, J.: Applying the new software engineering code of ethics to usability engineering: a study of 4 cases. J. Inf. Commun. Ethics Soc. **3**(3), 119–132 (2003)
22. Gotterbarn, D., Miller, K.: The public is the priority: making decisions using the software engineering code of ethics. IEEE Comput. **42**(6), 66–73 (2009)
23. Ferguson, S., Salmond, R., Al-Saggaf, Y., Bowern, M., Weckert, J.: The use of case studies in professional codes of ethics: the relevance of the ACS experience to ALIA's code of ethics. Aust. Libr. J. **54**(3), 299–308 (2005)
24. Maslin, M., Zuraini, I., Ramlah, H., Norshidah, M.: An ethical assessment of computer ethics using scenario approach. Int. J. Electron. Commer. Stud. **1**(1), 25–36 (2010)
25. Johnson, J.: Teaching ethics to science students: challenges and a strategy. In: Rappert, B. (ed.) Education and Ethics in the Life Sciences: Strengthening the Prohibition of Biological Weapons, pp. 197–213. ANU E Press, Canberra (2010)
26. Seach, G.R., Cattaneo, M., Burmeister, O.K.: Teaching ethics to IT practitioners. In: 6th International Conference of the Australian Institute of Computer Ethics, Burwood, Victoria (2012)