Department of Computer Science

Whither the privacy breach case studies?

Andrew Simpson

CS-RR-16-06

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

Whither the privacy breach case studies?

Andrew Simpson

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Abstract. Few weeks have passed in recent years without news of yet another data security breach that has the potential to impact upon the privacy of individuals. Following each event, there is significant coverage in both the mainstream media and the trade press; there is much hand-wringing; the organisation involved might be damaged (financially or reputationally, or both); there will be guesses as to the long-term effects on the individuals concerned; and then things move on ... until the next incident occurs, when the cycle is repeated. While some fields have a long-standing culture of learning lessons from disasters, giving rise to new and/or improved processes — both for the organisation itself and for the relevant sector as a whole — for a variety of reasons this is not the case in information security. We argue that a culture shift is necessary, and that the publication of well researched case studies describing privacy breaches, which has the potential to be impactful in a variety of ways, is well overdue.

1 Introduction

In recent years, few weeks have passed without news of yet another data security breach that has the potential to impact upon the privacy of individuals: this is a situation with which customers of Home Depot[1], eBay[2], Carphone Warehouse[3] and J.P. Morgan Chase[4] (amongst many others) will have some familiarity. In the USA this trend has given rise to new data breach disclosure laws in over 40 states[5]; in the UK this has (in part) made cyber security a strategic priority for the government[6]. There are web-sites dedicated to documenting and categorising such failures (see, for example, the Breach Level Index[7]), and there are annual surveys that provide awareness of risks and trends (see, for example,

[1] http://www.bbc.co.uk/news/world-us-canada-29946792
[2] http://www.bbc.co.uk/news/technology-27539799
[3] http://www.bbc.co.uk/news/uk-33835185
[4] http://www.bbc.co.uk/news/business-29470381
[5] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[6] https://www.gov.uk/government/policies/cyber-security
[7] http://www.breachlevelindex.com

the UK's Information Security Breaches Survey[8]). CNN Money has gone so far as to present US citizens with a 'What hackers know about you' tool[9].

While the received opinion is that things are getting worse, Edwards *et al.* [1] have found that neither the size nor the frequency of data breaches have increased over the past decade — although the potential harm is likely to be increasing [1]. Nevertheless, it is unarguable that we all — consumers; users; corporations; public sector organisations; governments; and individuals responsible for the design, development and deployment of software-based systems that deal with personal data — still have much to learn and improve upon.

Breach notification has a role to play in terms of information sharing and has arguably helped to improve processes (see, for example, [2–4]). Hausken [5] summarises how things have improved with respect to information sharing thus:

> "First, the US federal government encourages the establishment of Security Based Information Sharing Organizations (SB/ISOs) of various kinds, such as Information Sharing & Analysis Centers (ISACs), CERT, INFRAGARD, etc. Second, the 2002 Sarbanes-Oxley Act (SOX) places strict requirements on firms, such as ... establishing and maintaining adequate internal controls for financial reporting, and assessing annually the effectiveness of those controls." [5]

However, this is only a part of the solution. In particular, we would argue that there is still the need to learn from failure. This view is supported by Gal-Or and Ghose [6]:

> " ... it has been recognized that a key factor required to improve computer security is the gathering, analysis, and sharing of information related to successful, as well as unsuccessful, attempts at computer security breaches." [6]

Other disciplines have a culture of learning from failure. For example, Petroski's *To Engineer is Human: The Role of Failure in Successful Design* [7] and *Success through Failure: The Paradox of Design* [8] both have at their heart the sentiment that success comes from failure: by understanding the reasons for failure, engineers have been able to develop new designs, processes and solutions. Relatedly, examples of textbooks that focus on safety-critical systems that make good use of case studies include Leveson's *Safeware: System Safety and Computers* [9], Perrow's *Normal Accidents: Living with High Risk Technologies* [10], and *Learning from Disasters: A Management Approach* by Toft and Reynolds [11].

[8] `http://www.pwc.co.uk/industries/insurance/insights/2015-information-security-breaches-survey.html`

[9] `http://money.cnn.com/interactive/technology/what-do-hackers-have-on-you/`

While it is the case that many web-sites collate a great deal of information pertaining to data breaches[10] [11] [12] [13], and summaries of incidents are produced by Data Protection Commissioners[14] and Information Commissioners[15], there is not (for a variety of reasons) a culture of developing detailed academic case studies with a view to learning from data breaches. Indeed, the commercial sector has tended to take the lead in this respect: see, for example, the contributions of Experian[16] and PwC[17]. To quote Burkhead [12]:

> "While there is some fragmented literature addressing components of incident management for law enforcement and military organizations, there is a paucity of research addressing the management of information security incidents in private organizations from the experiences of corporate IT security professionals." [12].

(As an aside, it is important to recognise that such a tradition is developing in the broader cyber security context: see, for example, the consideration of the Maroochy Water Breach by Slaty and Miller [13] and the literature pertaining to Stuxnet [14–16]. In addition, David Wheeler's *Learning from Disaster* series of essays[18] is worthy of mention in this respect.)

In this paper, we give consideration as to why there is a lack of academic case studies in this area, and argue that there has to be change in this respect. We attempt to show how we might learn from failures — as the engineering discipline (as well as others) has done over many years. Our particular concern is data breaches that can lead to compromises of privacy. To this end, we adopt the definition of a *privacy incident* of Acquisti *et al.* [17]:

> "We broadly define a privacy incident as an event involving misuse of individuals' personal information. This misuse can consist of illegal sale, or usage, or lack of protection. It can be criminal, commercial, or ultimately innocuous. It can be intentional or unintentional. It can involve customers', partners', or employees' data." [17]

The structure of the remainder of this paper is as follows. In Section 2 we discuss our motivation. We then propose a modest research agenda in Section 3. We present conclusions in Section 4.

---

[10] http://www.databreaches.net
[11] http://www.privacyrights.org/data-breach
[12] http://www.breachlevelindex.com
[13] http://www.databreachwatch.org/
[14] https://www.dataprotection.ie/docs/Case-Studies/945.htm
[15] https://ico.org.uk/action-weve-taken/enforcement/
[16] http://www.experian.com/assets/data-breach/brochures/data-breach-lessons-learned-from-the-field.pdf
[17] http://www.pwc.com/us/en/forensic-services/assets/cyber-crime-data-breach-case-studies.pdf
[18] http://www.dwheeler.com/essays/learning-from-disaster.html

2 Data breaches, information sharing, and case studies

Much of modern business — indeed much of modern life — could not exist without data. Increasingly, data is omnipresent: commerce, education, finance and healthcare all increasingly have data at their heart. The importance of modern data security, together with increasing concerns about privacy due (in part) to the constant 'drip drip' of widely reported data breaches that can impact upon the security of personal information, makes for a complicated context.

Organisations that deal with personal data are obliged to deal with laws, regulations and guidelines that pertain to data protection. In the UK, relevant legislation includes the Data Protection Act[19], the Regulation of Investigatory Powers Act[20], and human rights legislation[21]. In the USA — which takes a sectoral approach — examples include the Health Insurance Portability and Accountability Act[22], the Sarbanes-Oxley Act[23], the Gramm-Leach-Bliley Bill[24], California Senate Bill Number 1386[25], and various state data breach disclosure laws.

When things do go wrong, they can impact in many ways. Acquisti *et al.* [17] argue that consumers can suffer thus:

- "The predominant harm for consumers following a breach is the risk of impersonation, fraud, or identity theft." [17]
- "Consumers suffer less tangible harms as well. Perceived privacy risk can be as important as real privacy risks, and demand commensurate protection ... so even the fear of privacy harms can be counted as a negative consequence of the loss of control and access restriction discussed above. Expectations matter, and the consumer suffers when they are violated." [17]

Acquisti *et al.* [17] go on to argue that firms can suffer thus:

- "In the US, the Federal Trade Commission ... can fine a firm responsible for breaches, or recommend expensive process overhauls to prevent future incidents." [17]
- "[Liability] is another consequence of privacy incidents that can become significant." [17]
- "[Notification] of affected consumers and accompanying recovery assistance such as a hotline represents non trivial expenses." [17]
- "An incident can damage a customer or partner relationship built on trust." [17]

[19] http://www.legislation.gov.uk/ukpga/1998/29/contents
[20] http://www.legislation.gov.uk/ukpga/2000/23/contents
[21] http://www.legislation.gov.uk/ukpga/1998/42/contents
[22] http://www.hhs.gov/ocr/privacy/
[23] http://www.soxlaw.com/
[24] http://www.banking.senate.gov/conf/confrpt.htm
[25] http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

– "Still, a firm might face higher insurance premia for liability after a breach, and future business partners might be less inclined to trust the firm." [17]

While there is a great deal of literature considering both the financial impact of data breaches (see, for example, the contributions of Campbell *et al.* [18], Garg *et al.* [19], Cavusoglu *et al.* [20], and Wang *et al.* [21], all of whom have documented the negative stock market impact of such incidents) and the economics of sharing information pertaining to information systems security (see, for example, the contributions of Gordon *et al.* [22], Gal-Or and Ghose [6], and Goode and Lacey [23]), there has been less consideration on the educational and instructional benefits of sharing such information. We would argue that breach disclosure — and related information sharing — is a starting point in terms of learning from failure. As an example, the Sarbanes-Oxley Act mentioned above encourages such sharing.

In Section 1 mention was made of the existence of web-sites that collate information pertaining to data breaches. One of the examples given was the Breach Level Index (BLI)[26], which was developed by Gemalto and SafeNet. The BLI categorises incidents in a variety of ways (organisation, location, industry, breach source, breach type, and number of records breached), and calculates a 'risk score' — a means of estimating breach severity on a scale from 1 to 10 — motivated thus:

> "By assigning a severity score to each breach, the BLI provides a comparative list of breaches, distinguishing nuisances from truly impactful mega breaches."

Scores are categorised as being one of: minimal (1–2.9); moderate (3–4.9); critical: (5–6.9); severe: (7–8.9); and catastrophic (9–10).

As another example, the Information Security Breaches Survey (ISBS, or 'Breaches Survey') is a series of reports commissioned by the UK's Department for Business, Innovation & Skills (BIS). Each report (see, for example, [24]) presents information about respondents, and summaries of data by, for example, type business, type of cyber security incident, and loss incurred. In addition, the data — in the form of anonymised responses — is made available[27]. The 2014 report [24] presents results from a survey conducted by PwC and follows the format of previous years in presenting an executive summary, followed by the main technical report itself. The main report presents the details behind the executive summary's highlights, and summarises information pertaining to the respondents, the data, the incidents, and the losses.

However, as useful as these contributions and resources are, there is no real opportunity to learn from failure. For example, as Tøndel *et al.* [25] argue, there are various motivations "for performing learning activities", including:

[26] `http://www.breachlevelindex.com`

[27] See `www.gov.uk/government/uploads/system/uploads/attachment_data/file/326419/information-security-breaches-survey-2014-technical-report-data.csv/preview` for the 2014 data.

– keeping security practitioners updated on current threats,
– getting new ideas on how to resolve challenging incidents,
– discussing possible improvements of the incident management process and its activities,
– performing trend analysis,
– identifying direct causes,
– identifying security measures that can prevent future incidents, and
– updating risk assessments of involved systems.

Similar motivations can be seen in relevant industry standards. For example, Point 16.1.6 of ISO/IEC 27002:2013 [26] (*Learning from information security incidents*) states:

> "Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents" [26].

ISO/IEC 27035 [27] expands upon the incident management controls of ISO 27002, breaking the process down into a series of steps, the last of which is "lessons learnt".[28] This step involves [25]:

– Performing further forensic analysis, if required
– Identifying lessons learnt
– Reviewing, updating and improving the implementation of security controls, the security incident management policy, and the organisations' existing risk assessment results
– Reviewing the effectiveness of the response process and procedures, as well as the reporting format and the organisational structure
– Updating incident and vulnerability databases
– Sharing review results within a trusted community

Fundamentally, this activity can: eliminate (or, at least, reduce) the likelihood of the event (or similar events) happening again; indicate new threats and the need to revise threat models; and help to improve processes and structures. Crucially, ensuring a successful outcome requires an understanding of exactly what happened and why.

There is evidence, though, that incident response is insufficient. For example, Jaatun *et al.* [31], who in describing the findings of a series of interviews, argue:

> "The learning phase after an incident was considered to be important by the interviewees. However, some interviewees were unsure if learning actually has any effect on future activities, and they feared that learning is quickly forgotten. Root causes are not always identified, discussions do not always involve ICT and process professionals, and lessons learned are not published." [31]

[28] Other guidelines that concern themselves with incident management include those of NIST [28], ENISA [29], and SANS [30].

We would argue, therefore, that well researched, peer-reviewed case studies concerned not just with the impact, but — more importantly — with the causes, of privacy breaches have a greater role to play in the academic discourse in this area than has hitherto been the case.

Yin [32] defines a case study as an "empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" [32]. Case studies are generally agreed to be a good educational tool [33–36].

In our context, case studies have the potential to provide benefits to a wide variety of stakeholders. While there is a long tradition of case studies in information security research (see, for example, [37–39]), there is no such tradition when it comes to security incidents, as observed by Burkhead [12] amongst others (including Kadlec and Shropshire [40], Rajakumar and Shanthi [41], and Werlinger *et al.* [42]). Reasons postulated for this include:

- "Firms naturally find incentives to invest in security technology, but incentives for information sharing are harder to furnish." [5]
- "Information security research is one of the most intrusive types of organization research, and there is undoubtedly a general mistrust of any 'outsider' attempting to gain data about the actions of the security practitioner community." [43]
- "Firms will not share information that may be considered harmful without getting assurances, and provide insights with regard to how to improve their organization." [44]

There would, though, be clear benefits. To quote Smith *et al.* [45]:

> "At the organizational level, an interesting contribution would be to reveal specific organizational outcomes and consequential decisions made after breaches of personal information considered private" [45].

3 A modest research agenda

In this section, we outline a modest research agenda. In particular, we characterise three classes of contributions.

3.1 Individual breaches: building on exemplars

In addition to sources identified earlier in this paper (and, indeed, others, such as CERT [29]), some examples of case studies do exist. For example, in the UK, the Office of the Information Commissioner has produced a series of case studies detailing action which that office has taken[30]; examples of case studies are available from the SANS Institute web-site[31]; from a business perspective, we find

[29] `http://www.cert.org/`
[30] `https://ico.org.uk/action-weve-taken/case-stories/`
[31] `https://www.sans.org/reading-room/whitepapers/casestudies`

a series of case studies from Harvard Business School — pertaining to, for example, ChoicePoint [46], TJZ [47], and Sony [48]. All of these have their merits; however, they do not provide the forensic analysis that might be beneficial to information security researchers and practitioners to benefit from the "learning from information security incidents" philosophy of ISO/IEC 27002:2013. Taking any of these as a starting point and trying to understand precisely what happened — from a process and/or technical standpoint — and identifying the lessons that might be learned would be beneficial.

3.2 Sectoral studies

The USA, in particular, has taken a sectoral approach to data security; as such, there may be merit in taking a sector-by-sector approach to establishing a body of literature.

For all sorts of reasons, media sources tend to focus on data breaches that involve big corporations: those that impact, for example, large financial organisations, large media organisations, or large retailers. This might be because the breaches and the nature of the data make the story accessible; it might be because the potential impact is significant. Nevertheless, there is one sector that has seen a steady stream of data breaches with little coverage in the mainstream media — education.

The scale is significant:

> "30 educational institutions [in the USA] experienced data breaches in 2014. Five of the thirty schools actually had larger data breaches than the notorious Sony Hack." [49]

Further, it has been estimated that higher education institutions are responsible for 35% of all security breaches in the USA [50]. It might be argued that targeting such institutions for criticism is unfair as the culture of openness and transparency means that more breaches are more likely to be disclosed, resulting in statistical bias.

Writing in 2009, Cline [51] claimed that: "According to my records, over 300 publicized privacy incidents have occurred at U.S. institutions of higher learning since 2001, with at least 53 colleges and universities experiencing multiple breaches" [51]. (Cline had written about the issue four years previously, identifying higher education as the primary sector for publicised data breaches [52].)

In fairness, it should be noted that this is not just an issue for the USA; UK universities have also been affected. For example, the personal data of 148 students — including mobile phone numbers and addresses — was accidentally made accessible via a student inquiry page at the University of York's website.[32] According to the aforementioned Breach Level Index, as of October 2nd, 2015, the 'top' fives data breaches in this sector in the UK are as documented in Table 1.

[32] See `http://www.bbc.co.uk/news/uk-england-york-north-yorkshire-12756951`.

Organisation	Date	# records	Breach source	Breach type
Staffordshire University	Oct. 2014	125,000	Malicious outsider	Account access
University of Nottingham	May 2014	4,751	Accidental loss	Identity theft
Brunel University	Mar. 2015	61	Accidental loss	Existential data
University of Bedfordhsire	August 2015	50	Accidental loss	Identity theft
University of Birmingham	April 2015	Unknown	Malicious outsider	Existential data

Table 1. 'Top 5' UK HEI data breaches, according to `http://breachlevelindex.com`

3.3 Partitioning by type

Rather than breaking down the universe of problems on a sectoral basis, there may be merit in breaking down the universe by 'type of incident'. The taxonomy of Ayyagari [53] — whereby incidents are classified in terms of the categories "unintended disclosure", "hacking or malware", "payment card fraud", "insider", "physical loss", "portable device" and "stationary device" — may be beneficial in identifying lessons. A further motivation for this would be that previous research on the (financial) impact of incidents has adopted such categorisations.

4 Conclusions

In this paper, we have given consideration to privacy incidents — data breaches that can lead to compromises of personal information. While breach notification is one part of the information-sharing process following such incidents — and has been beneficial in and of itself [3, 4] — we have argued that case studies have a greater role to play than has hitherto been the case. To quote Thomas *et al.* [54], "it will not be possible to achieve collective security outcomes without disclosure and sharing other information regarding security" [54].

The potential benefits are significant: insights into the nature of incidents can be established and trends can be identified. Both researchers and practitioners stand to benefit, as do those responsible for drawing up policies, both within individual organisations, and at sectoral and national levels.

There will be hurdles to be overcome: there is a need for good access to information and resources (Sohail [55], Rees and Kannan [56], and Crossler *et al.* [39] have all demonstrated the reluctance of companies to disclose information related to such incidents); organisations will need concrete guarantees that any information sharing will not lead to additional compromises or harm; the motivation and incentives — both for researchers and cooperating organisations — will need to be clear. Further, case studies have their limitations (see the

contributions of Diefenbach [57] and Blichfeldt and Andersen [58], which consider some arguments against case studies). However, we would argue that an approach that has improved processes and technologies — and, ultimately, safety — in a wide variety of industries — often involving companies that are competitive and secretive — has more to offer in helping us to learn more about (and from) privacy incidents than has hitherto been the case.

References

1. Edwards, B., Hoffmeyr, S., Forrest, S.: Hype and heavy tails: A closer look at data breaches. In: Proceedings of the 14th Annual Workshop on the Economics of Information Security (WEIS 2015). (2015)
2. Gordon, L.A., Loeb, M.P., Lucyshyn, W., Sohail, T.: The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. Journal of Accounting and Public Policy **25**(5) (2006) 503–530
3. Bisogni, F.: Data breaches and the dilemmas in notifying customers. In: Proceedings of the 14th Annual Workshop on the Economics of Information Security (WEIS 2015). (2015)
4. Laube, S., Böhme, R.: The economics of mandatory security breach reporting to authorities. In: Proceedings of the 14th Annual Workshop on the Economics of Information Security (WEIS 2015). (2015)
5. Hausken, K.: Information sharing among firms and cyber attacks. Journal of Accounting and Public Policy **26**(6) (2007) 639–688
6. Gal-Or, E., Ghose, A.: The economic incentives for sharing security information. Information Systems Research **16**(2) (2005) 186–208
7. Petroski, H.: To Engineer Is Human: The Role of Failure in Successful Design. Vintage Books (1992)
8. Petroski, H.: Success through Failure: The Paradox of Design. Princeton University Press (2008)
9. Leveson, N.G.: Safeware: System Safety and Computers. Addison-Wesley (1995)
10. Perrow, C.: Normal Accidents: Living with High Risk Technologies. Princeton University Press (1999)
11. Toft, B., Reynolds, S.: Learning from Disasters: A Management Approach. 3rd edn. Palgrave Macmillan (2005)
12. Burkhead, R.L.: A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management. PhD thesis, Capella University (2014)
13. Slay, J., Miller, M.: Lessons learned from the Maroochy water breach. In Goetz, E., Shenoi, S., eds.: Critical Infrastructure Protection. Volume 253 of IFIP International Federation for Information Processing. Springer (2008) 73–82
14. Chen, T.M., Abu-Nimeh, S.: Lessons from Stuxnet. Computer **44**(4) (2011) 91–93
15. Langner, R.: Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy **9**(3) (2011) 49–51
16. Collins, S., McCombie, S.: Stuxnet: The emergence of a new cyber weapon and its implications. Journal of Policing, Intelligence and Counter Terrorism **7**(1) (2012) 80–91
17. Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? An event study. In: Proceedings of the 27th International Conference on Information Systems (ICIS 2006). (2006)

18. Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L.: The economic cost of publicly announced information security breaches: Empirical evidences from the stock market. Journal of Computer Security **11**(3) (2003) 431–448
19. Garg, A., Curtis, J., Halper, H.: Quantifying the financial impact of IT security breaches. Information Management & Computer Security **11**(2) (2003) 74–83
20. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce **9**(1) (2004) 69–105
21. Wang, T.W., Rees, J., Kannan, K.: Reading the disclosures with new eyes: Bridging the gap between information security disclosures and incidents. In: Proceedings of the 7th Workshop on the Economics of Information Security (WEIS 2008). (2008)
22. Gordon, L.A., Loeb, M.P., Lucyshyn, W.: Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy **22**(6) (2003) 461–485
23. Goode, S., Lacey, D.: Social embeddedness and sharing security information: Bridging the cost benefit gap. In: Proceedings of the 20th Australasian Conference on Information Systems (ACIS 2009). (2009)
24. Department for Business, Innovation and Skills: Information Security Breaches Survey 2014. `https://www.gov.uk/government/publications/information-security-breaches-survey-2014` (2014)
25. Tøndel, I.A., Line, M.B., Jaatun, M.G.: Information security incident management: Current practice as reported in the literature. Computers & Security **45** (2014) 42–57
26. ISO/IEC: Information technology – security techniques – code of practice for information security management. ISO/IEC 27002:2013 (2013)
27. ISO/IEC: Information technology – security techniques – information security incident management. ISO/IEC 27035:2011 (2011)
28. Grance, T., Kent, K., Kim, B.: NIST SP 800-61: Computer Security Incident Handling Guide. National Institute of Standards and Technology (2008)
29. European Union Agency for Network and Information Security (ENISA): Good practice guide for incident management. `https://www.enisa.europa.eu/activities/cert/support/incident-management` (2010)
30. Kral, P.: The Incident Handler's Handbook. SANS Institute (2011)
31. Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A., Longva, O.H.: A framework for incident response management in the petroleum industry. International Journal of Critical Infrastructure Protection **2**(1–2) (2009) 26–37
32. Yin, R.: Case study research: Design and methods. 2nd edn. Sage Publications (1994)
33. Feagin, J.R., Orum, A.M., Sjoberg, G., eds.: A Case for the Case Study. UNC Press Books (1991)
34. Rowley, J.: Using case studies in research. Management Research News **25**(1) (2002) 16–27
35. Gerring, J.: Case Study Research: Principles and Practice. Cambridge University Press (2007)
36. Simons, H.: Case Study Research in Practice. SAGE Publications (2009)
37. Cavaye, A.L.M.: Case study research: A multi-faceted research approach for IS. Information Systems Journal **6**(3) (1996) 227–242
38. Darke, P., Shanks, G., Broadbent, M.: Successfully completing case study research: Combining rigour, relevance and pragmatism. Information Systems Journal **40** (1998) 273–289

39. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security **32**(1) (2013) 90–101
40. Kadlec, C., Shropshire, J.: Best practices in IT disaster recovery planning among US banks. Journal of Internet Banking & Commerce **15**(1) (2010) 1–11
41. Rajakumar, M., Shanthi, V.: Security breach in trading system countermeasure using IPTraceback. American Journal of Applied Sciences **11**(3) (2014) 492–498
42. Werlinger, R., Muldner, K., Hawkey, K., Beznosov, K.: Preparation, detection, and analysis: The diagnostic work of IT security incident response. Information Management & Computer Security **18**(1) (2010) 26–42
43. Kotulic, A.G., Clark, J.G.: Why there aren't more information security research studies. Information & Management **41**(5) (2004) 597–607
44. Zafar, H.: Security risk management at a fortune 500 firm: A case study. Journal of Information Privacy and Security **7**(4) (2011) 23–53
45. Smith, H.J., Dinev, T., Xu, H.: Information privacy research: An interdisciplinary review. MIS Quarterly **35**(4) (2011) 989–1016
46. Sharp Paine, L., Phillips, Z.: ChoicePoint (A). Harvard Business Review # 306001 (2006)
47. Haggerty, N.R.D., Ramasastry, C.S.: Security breach at TJX. Harvard Business Review # 908E03 (2008)
48. Seijts, J., Bigus, P.: Sony PlayStation: Security breach. Harvard Business Review # W12309 (2012)
49. McCarthy, K.: 5 colleges with data breaches larger than sony's in 2014. `http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html` (2015)
50. Barker, I.: 35 percent of all security breaches take place in higher education. `http://betanews.com/2014/12/17/35-percent-of-all-security-breaches-take-place-in-higher-education/` (2014)
51. Cline, J.: What's behind the rash of university data breaches? `www.networkworld.com/news/2009/030909-whats-behind-the-rash-of.html` (2009)
52. Cline, J.: Security breaches challenge academia's 'open society'. `www.computerworld.com/s/article/102298/Security_breaches_challenge_academia_s_open_society_` (2005)
53. Ayyagari, R.: An exploratory analysis of data breaches from 2005–2011: Trends and insights. Journal of Information Privacy and Security **8**(2) (2012) 33–56
54. Thomas, R.C., Antkiewicz, M., Florer, P., Widup, S., Woodyard, M.: How bad is it? — a branching activity model to estimate the impact of information security breaches. In: Proceedings of the 12th Annual Workshop on the Economics of Information Security (WEIS 2013). (2013)
55. Sohail, T.: To tell or not to tell: Market value of voluntary disclosures of information security. PhD thesis, University of Maryland (2006)
56. Rees, J., K., K.: Reading the disclosures with new eyes: Bridging the gap between information security disclosures and incidents. In: Proceedings of the 7th Workshop on the Economics of Information Security (WEIS 2008). (2008)
57. Diefenbach, T.: Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews. Quality & Quantity **43**(6) (2009) 875–894
58. Blichfeldt, B.S., R., A.J.: Creating a wider audience for action research: Learning from case-study research. Journal of Research Practice **2**(1) (2006) 1–15