# Modelling Trust and Trust-Building Among IT-Security Professionals

## How Do Practitioners Find Out Whom to Work With?

Laurin B. Weissinger(✉)

Nuffield College, University of Oxford, Oxford, UK
Laurin.weissinger@nuffield.ox.ac.uk

**Abstract.** By analysing cyber-security as a private protection market, and linking it with technological aspects and the dominating risk-environment, valuable insights into its workings can be gained, particularly when it comes to non- or semi-technical factors. Using high-granularity, empirical interview data ($n = 140$) as input, this paper presents insights about trust, signalling and cooperation among practitioners in the context of a complex field. At the moment, trust-building in the cyber-protection business is very personalised. Due to complexity and uncertainty, cooperation is based on social networks and reputation, while institutional signals are less significant than in other high-risk areas. While more research is necessary to unpack this issue, the analysis provides some understanding of how the field and technological aspects shape protection-market conditions, and how preferences regarding signalling and assessment change in practice according to the actors and organisations involved in a given situation. Evaluating other actors is generally based on above-mentioned personal factors, rather than institutional signalling.

## 1 Protection and Cooperation in IT-Security

IT-Security is complex, decentralised, and predominantly privately ordered [1, p. 13], [2, p. 272]. This makes judging other actors, human and organisational, an important aspect of IT-Security provision. This paper draws from analytical sociology [3–5], signalling theory [6–8], and studies about protection-markets [9–11] to contribute an understanding of trust-building in cyber-protection that is focussed on the human side of the equation. If tasks are diverse and actors depend on each other to ensure overall functionality, both within and across organisations, *organic* conditions are given [12, chap. 3], [13, pp. 315ff], [14, pp. 19ff]. This means that different centres of expertise must cooperate to keep the system running. Information technology and security are a prime example for such conditions: Actor $A$, Alice, requires her machines and networks to run smoothly, and consequentially must be confident that other actors, e.g. Bob ($B$), behave as promised or expected. Alice has two ways to build confidence: control or trust [15, p. 4].


T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 557–566, 2017.
DOI: 10.1007/978-3-319-58460-7_39

The *traditional* strategy in modernity has been control-focussed and bureaucratic, *guaranteeing* compliance through audits and standardisation [13, pp. 14ff], [16, pp. 6–8]. Institutional trust, embodied in rules [13, p. 68], is given to regulators, which govern a certain *domain* by testing, auditing, and certifying products and people [15, p. 32], [16]. This top-down system is based on uniformity and non-dyadic *system trust* [14, pp. 16–17]. Control-strategies increase predictability by reducing individual agency and expectable errors [17, p. 128], which helps to mitigate anticipatable risks [18]. Yet, rigid regimes struggle with *Unknown Unknowns* [19, p. 335] that are common in IT-Security due to the complexity of interconnected components and systems: Alice is confronted with a nearly unlimited number of (potential) threats and weaknesses. With third party enforcement – e.g. by states – currently lacking, cybersecurity is defensive and specific: cyber-protectors use counter-measures that are difficult to test and never perfect [20, p. 208]. The strongest security solution wins, while the weakest link, if human or technological, defines system security [20, p. 114].

To succeed in building and maintaining a functional security architecture, cyber-protectors, i.e. those individuals actively trying to prevent harm by ensuring confidentiality, availability, and integrity,[1] and their clients must cooperate [21, p. 239], [22, pp. 27ff]. This setup demands interpersonal or intra-organisational trust between high-level experts. Generally, managing and anticipating risks, securing systems, and evaluating people are uncertain processes, based on *internalised learning processes* and *heuristics* [18], [23, p. 24], [24, p. 40], [25] but in IT-Security, the trust game is particularly difficult: First, cyber-attacks and vulnerabilities are usually harder to detect than physical ones. Second, networks grow and evolve quickly, escaping standardisation. Inappreciable disparities can compromise networks, while one vulnerable component can affect millions of machines and users (e.g. *Hearthbleed* bug). Third, alongside networks and systems, attack- and defence-strategies change rapidly, causing ever-unfolding imbalances [20, pp. 73ff, p. 89]. Last but not least, cyber-protection is necessarily multi-dimensional. Various resources and types of expertise are needed to establish protection.

In consequence, collaboration and using other people's work is the only rational option to reach an acceptable level of security: trusting Bob reduces the scenarios Alice must take into account. For example, if Alice is sufficiently confident that Bob's code is error-free, she will discard some attack-scenarios. To gain this sufficient confidence in Bob's abilities and trustworthiness, Alice, as assessor, interprets signals emitted by Bob, signals emitted by others about Bob, and recorded past signals to form her beliefs about him. Based on this imperfect information and the given situation, Alice judges if Bob is sufficiently unlikely to defect or fail in future cooperation, i.e. she forms

*a hypothesis of future behaviour that is located between knowing and not knowing, but an assumption held with enough confidence to base practical action on.* [26, p. 346]

[1] e.g. Analysts, Penetration Testers, Security Architects.

Yet, as Alice starts trusting, her dependence becomes a risk; and while trustworthy entities do not fail, failing trusted entities compromise security [27, p. 13]. In consequence, Alice will try her best to cooperate with actors that are both trustworthy and sufficiently skilled. Much work has been done in the security field about managing trust but trust and trust-building, particularly in the social realm, have remained black boxes [3, pp. 27ff]. This paper discusses one important aspect, namely how signalling and assessment-processes feed into beliefs [24, p. 29]:

*How can an agent, the receiver, establish whether another agent, the signaller, is telling or otherwise conveying the truth about a state of affairs or event, which the signaller might have an interest to misrepresent? And, conversely, how can the signaller persuade the receiver that he is telling the truth, whether he is telling it or not?* [28, p. 168]

In line with the theory [13,14,23,29–31], it seems that market conditions and technological aspects in cyber-security increase the importance of trust vis-à-vis control. Cooperation-ties with autonomous experts in critical fields are always hazardous [32, p. 214], but particularly so in security, where protectors need a lot of privileges and insights. In IT-Security, testing prowess is difficult for a variety of reasons, as institutional signalling or embeddedness are usually deficient [33]: many cyber-protectors lack official certifications and there are no strong associations with signalling power between officially sanctioned certifications or memberships, and the individual, hidden properties of sufficient skill and particularly trustworthiness. Thus, this paper hypothesises:

$H_{1a}$ A more individually-focussed process than in other high-security, high-discretion sectors is expected.
$H_{1b}$ Actors will prefer personal and network-based assessment over institutionally-based signals.
$H_{1c}$ Homophily, continued interaction and reciprocity will strengthen ties.
$H_2$ Reputation is central, as demonstrating fundamental qualities is costly (skill) or impossible (trustworthiness).

## 2 Methodology

This paper is based on 140 research interviews with cyber-protectors, whose identities cannot be revealed. Individuals were sampled from a variety of industries and countries. In terms of experience and skill, the main focus was on people with considerable experience (five years or more) and/or expertise. Nevertheless, some less experienced individuals were interviewed to avoid an overly biased sample. In terms of geography, most interviewees were either European or from North America, with some people from Latin America, and fewer Asians and Africans. Most people in the sample work for smaller employers, particularly penetration testers and consultants, while some, for example security architects, predominantly worked for large corporations. Interviews were in-depth and comprehensive, usually taking between 45–70 min.

Due to the aims of this paper, expert interviews were the most suitable data source. Yet, the interviewees represent a small, potentially non-random sample of the target population [34, pp. 56–59], [35, p. 124] and thus external validity is difficult to establish. Due to misrepresentation and misunderstandings, the findings could therefore be affected by *systematic measurement errors* [35, p. 156]. On the other hand, expert interviews are most appropriate. Firstly, personal contact was necessary to establish trust and legitimacy [34, pp. 64–65]. Second, the *microanalysis of processes* [36, pp. 58–59] requires dialogue, like the use of examples and hypothetical scenarios. Third, as this study tries to develop a model and understanding [17, p. 4], [32], empirical evidence directly feeds into the model, requiring interactivity and flexibility [36, p. 98]. Fourth, the research problem is multi-faceted [37, p. 190], which, at the outset, is best approached qualitatively [34, see p. 8]. Internally, conclusions seem valid: people in different positions, companies, and fields from a variety of different backgrounds presented similar interpretations of the field, which were also in line with the sociological and security literatures [38, see pp. 312–315].

The interviews focussed on the questions of trust and cooperation. The main goal was to grasp the way the interviewees tried to ensure that they were working with trustworthy contacts, and exploring how they would go about finding individuals with specific skills. For example, how would they try to get a feel for another person, what would they do to avoid being manipulated or conned, what types of information would they focus on, and where would they acquire this information? The main focus of the analysis was then to understand the perceptions and preferences of the interviewees but also to develop a basic, yet functional model of how these perceptions influence decision-making when it comes to hiring and cooperation. This was achieved using a *Content Analysis* methodology, i.e. by systematically interpreting, coding, systematising, and finally quantifying the interpretations and preferences expressed in the interviews.

## 3 Model and Findings

### 3.1 Main Assessment Factors and Decision Model

Cyber-security is a complex market with little external enforcement, which influences what actors consider *subjectively rational* [32, p. 136]. As in Spence [39, pp. 360–361], [40, p. 455], non-cooperation is an option per individual evaluation process but actors must choose *someone* and determine their trustworthiness correctly. Decisions result from belief-based, rationalising thought-processes [41, p. 4], within the limits imposed by empirical reality. The data indicate that cyber-security experts do actively research and weight different kinds of evidence and signals to decide if they want to cooperate. Formally, the decision to cooperate ($D$) is based on the believed probability $p$ of success times the expected benefits, minus the probability $(1-p)$ of failure multiplied by the expected costs [42, see p. 394], and [32, chap. 9]. As this is a decision making process, $p$ is not equivalent to the real probability, but represents beliefs. The assumed probability

of success is based on a function ($f$) of the assessment of skills and trustworthiness, with $C$ denoting confidence-levels. Both confidence levels, $C_{Skill}$ and $C_{Trustworthiness}$, are based on beliefs resulting from signals received.

$$D_{Cooperation} = (p \times Benefits) - (1 - p \times Costs)$$

with

$$p = f(C_{Skill} \times C_{Trustworthiness})$$

The interviews show that $C_{Skill}$ and $C_{Trustworthiness}$ are dependent on eight main factors, of which some are more decisive than others, yet further research is needed to understand and analyse their relative importance in different situations.

- Intentional Signalling, i.e. what actors tell others openly through speech, written text, or otherwise.
- Unintentional Signalling, i.e. signals sent out unwillingly, e.g. signs of stress, accent, habitus.
- Interpersonal Histories, i.e. a shared past with the assessee.
- Official Qualifications, e.g. degrees, certifications.
- Artefacts, i.e. remainders of activity on the internet, e.g. published papers, blogs, or code on github.
- Professional Associations, e.g. membership in the $(ISC)^2$.
- Group Affiliations, e.g. ex-hacker, ex-criminal, nationality, etc.
- Social Networks, e.g. shared professionals contacts, or friends.

The interviews further indicate that the weighting of these factors is variable: personal preferences ($\alpha$) regarding different signalling types ($\delta_x$), organisational preferences or rules ($\beta$), and situational factors ($\gamma$) influence the way the assessment is made. While input signals and evaluation procedures differ, the function is the same for both $C_{Skill}$ & $C_{Trustworthiness}$.

$$\begin{aligned} C = {} & (\alpha_1 + \beta_1 + \gamma_1) \times \delta_{Intent.Sig.} + (\alpha_2 + \beta_2 + \gamma_2) \times \delta_{Unintent.Sig.} \\ & + (\alpha_3 + \beta_3 + \gamma_3) \times \delta_{Interpers.Hist.} + (\alpha_4 + \beta_4 + \gamma_4) \times \delta_{Qualifications} \\ & + (\alpha_5 + \beta_5 + \gamma_5) \times \delta_{Artefacts} + (\alpha_6 + \beta_6 + \gamma_6) \times \delta_{Prof.Assoc.} \\ & + (\alpha_7 + \beta_7 + \gamma_7) \times \delta_{Group\,Aff.} + (\alpha_8 + \beta_8 + \gamma_8) \times \delta_{Soc.Netw.Sig.} \end{aligned}$$

The outcome $C$ would be an assumed trustworthiness- or skill-level, ranging from absolute confidence to none.[2] How strongly preferences and external factors, $\alpha$, $\beta$ & $\gamma$, influence the overall multiplicator depends on the relative power of their source: bigger organisations are more influential in rule-setting, while powerful individuals have more discretion.

Unlike in other domains, usually influential aspects, like demographic factors, locality, and nationality[3] are not salient. However, interviewees note that it is

[2] With $\sum \alpha_{1-8} = \alpha_{total}$.
[3] With some exceptions.

easier for them to judge socially similar actors [43, p. 435]. Dyadic homophily increases inter-personal understanding but also the likelihood of having access to triadic relationships, which directly or indirectly, passively or actively *vouch* for the other party. Second, market-conditions and interactions are formative, unlike nationality or geographical location. Generally, cyber-protectors prefer evidence-based trust, or at least an approximation thereof; a *lack of contrary evidence* [6, p. 234] is not enough. As hypothesised, the process among experts is very individualised and specific. Someone doing general website-security can accept higher risks than cyber-protectors of a defence company; the latter's confidence, $C$, must be much higher to accept cooperation.

### 3.2 Illustrative Example

Let it be assumed that Alice is an IT-Security professional who requires Bob's services, specifically his expertise in cryptography. Alice herself is specialised in computer networking and does not have the needed expertise, nor the time and resources to obtain them. Alice who works in a small security consultancy will try to find suitable candidates within her close social network, preferably someone she already knows personally and has worked with in the past. That failing, Alice will try to find Bob within her wider social network, i.e. asking her contacts for recommendations and ideas, with a preference for those colleagues and friends that she knows best and trusts the most. Based on these recommendations from the social network, Alice could then draw up a short-list, again with a strong preference for people she already knows, or people that her most trusted contacts know and can vouch for.

In all likelihood, Alice will try to gain insight into Bob's work; e.g. if he has published papers or code online, scanning these artefacts for evidence of Bob's skill. In addition, she may read and analyse his communications, say on an online forum to get a better *feel* for him. Interviews are likely to be significant to Alice, both to listen to what Bob has to say, and to test him as much as she can. As the interviewees report, good questions and challenges will provoke insightful answers that allow them to get a good grasp of candidates and potential partners. Face-to-face encounters are also important to Alice. These create many unintentional signals that Alice can analyse. What Alice would be looking for specifically depends on the situation ($\gamma$) and preferences ($\alpha, \beta$) but she will likely focus on signs of betrayal, on the (in-)ability to work under stress, and on inconsistencies in what is being said and Bob's non-verbal signalling, i.e. his behaviour more generally. Group affiliations are usually less important as signals but may be relevant, particularly if Bob has a background that could be associated with criminality or foreign powers.

All these signals and factors would also play into the selection of doctors, pilots, or lawyers. The main difference is that in these cases, there would be an *un-circumventable* pre-selection rule-set related to officially sanctioned qualifications like degrees, and professional associations, e.g. boards, which are based on testing and/or other conditions of membership. Cyber-protectors often struggle to demonstrate their prowess in the way that other professions can.

Unlike cyber-protectors, surgeons can refer to photographic evidence, pilots can show their service and training record, and lawyers can refer to cases they have won. This lack of powerful signalling devices in IT-Security is due to strong secrecy specifications and non-disclosure agreements, and because there are no general pre-selection rule-sets as in areas like medicine or law.

While it is true that some positions require certain credentials, commonly the CISSP, the interviewees did not discuss this aspect in much detail. Rather, they expressed the opinion that a CISSP can be held by individuals with little skill, due to its high-level, theoretical nature. Another aspect that was only discussed in passing were security clearances and background checks. Firstly, most interviewees were or are employed in private industry, and those that had been cleared or checked did not consider this an important element of assessing other people when it comes their *trustworthiness* or *skill*. Rather, they saw this as a necessary step after their selection had been made to confirm eligibility, satisfy requirements, and mitigate risks going forward.

Last but not least, it is important to note that Alice's preferences may be overwritten by her organisation, or the situation. Due to the regulative environment, compliance likely trumps security in an organisational context. While such requirements were often considered to have only limited impact on actual security and trustworthiness, they do increase the salience of certifications in the selection process. If problems arise, the ability to present credentials and demonstrate *due diligence* may be more important than a functional security environment. Thus, the objectives of security actors are potentially in-congruent with the aims of their employer. Alice's situation is also crucial to the evaluation process: the more pressing the circumstances and the higher the payout vs. the potential losses, the more leeway she will – or be ordered to – allow. Particularly in combination with above-mentioned organisational requirements, this can lead to incentives and strategies that are unaligned with the goal of increasing security.

### 3.3 Hypotheses and Empirical Insight

It is nearly impossible to unequivocally signal trustworthiness or skill in the professional sphere of IT-Security, as cheating is comparatively easy and because there is little enforcement in general. With institutional signals that dominate other professional fields being largely absent, the evaluation of alters is mainly individual and specific, on a case-by-case basis ($H_{1a\&b}$). Having, and retaining, a good reputation is immensely important ($H_2$) and security professionals strongly prefer using their social networks and contacts to find new colleagues or partners. As expected in more or less any social network, homophily ($H_{1c}$) facilitates trust-building. The sources indicate that they have an easier time gauging individuals from backgrounds similar to their own. Yet, they claim – and appear – to not exclude individuals based on their nationality, past, or other types of group belonging. In contrast to other high-risk domains, assessment appears to be more thorough and personalised, while control efforts appear less useful. Yet, more research is necessary to explain and link the factors presented above.

The reasoning behind interviewees' preferences appears to be associated with the uncertainties experts face due to the lack of trusted institutions or enforced regulation regimes.

## 4 Conclusion

At this time, protection in cyberspace is necessarily private, defensive and particular, as there are no authoritative institutions that can settle disputes and enforce decisions. Technology and the cyber-protection market condition the importance of trust and reputation, and strongly influence the way trust is assessed and signalled in the field. When hiring an accountant or doctor, the foremost criterion is official recognition. For most IT-Security professionals in the sample, this pre-selection criterion is usually absent.

In the technological realm, confidence-building is based on control and trust. Yet, socially and among experts in particular, control is often difficult to employ as a guarantor for compliance. Trust can hardly be replaced, due to IT-Security's complexity and interconnectedness: there is no other way but to trust complex technical systems, contractors, one's own team or employees, as well as the general infrastructure. The interviews are congruent in supporting the hypotheses: the evaluation and *testing* of other actors is based on personalised processes, reputation seems to matter a lot, and the eight factors described are considered central. As underlined, further research is necessary to unpack the concepts, their relationships, and interconnectedness, as well as their relative importance in different situations. In many ways, trust-building in cyber-security appears to be procedurally similar but more extreme than trust-building elsewhere. In a nutshell, cyber-protectors prefer and are compelled by the IT-security domain to find out whom to work with by thoroughly looking into every possible co-operator, their past, their available work and skills, as well as their social networks. However, fully understanding how assessment in the sector could be streamlined or improved would necessitate further research into this area.

## References

1. Kobayashi, B.K.: Private versus social incentives in cybersecurity: law and economics. In: Grady, M.F., Parisi, F. (eds.) The Law and Economics of Cybersecurity. Reissued, pp. 13–28. Cambridge University Press, Cambridge (2011)
2. Trachtman, J.P.: Global cyberterrorism, jurisdiction, international organization. In: Grady, M.F., Parisi, F. (eds.) The Law and Economics of Cybersecurity. Reissued, pp. 259–296. Cambridge University Press, Cambridge (2011)
3. Hedström, P.: Dissecting the Social: On the Principles of Analytical Sociology, 188 p. Cambridge University Press, Cambridge (2005)
4. Elster, J.: Explaining Social Behavior: More Nuts and Bolts for the Social Sciences, 1st edn., 496 p. Cambridge University Press, Cambridge (2013)
5. Hedström, P., Bearman, P.: The Oxford Handbook of Analytical Sociology, 800 p. Oxford University Press, Oxford (2009)

6. Gambetta, D.: Trust: Making and Breaking Cooperative Relations, 1st edn., 280 p. Wiley-Blackwell, New York (1988)
7. Gambetta, D.: Codes of the Underworld: How Criminals Communicate, 368 p. Princeton University Press, Princeton (2009)
8. Goffman, E.: Behavior in Public Places: Notes on the Social Organization of Gatherings. Reissued, 258 p. Free Press, New York (2008)
9. Varese, F.: The Russian Mafia: Private Protection in a New Market Economy. New edition, 306 p. Oxford University Press, Oxford (2001)
10. Varese, F.: Mafias on the Move: How Organized Crime Conquers New Territories. Reprint, 284 p. Princeton University Press, Princeton (2011)
11. Gambetta, D.: The Sicilian Mafia: The Business of Private Protection, New edition, 346 p. Harvard University Press, Cambridge (1993)
12. Durkheim, E.: The Division of Labour in Society, New edition, 412 p. Palgrave Macmillan, Basingstoke (1984)
13. Fox, A.: Beyond Contract: Work, Power and Trust Relations, 408 p. Faber & Faber, London (1974)
14. Lane, C., Bachmann, R.: Trust within and between Organizations, 334 p. Oxford University Press, Oxford (1998)
15. Cofta, P.: Trust, Complexity and Control: Confidence in a Convergent World, 1st edn., 310 p. Wiley-Blackwell, Chichester (2007)
16. Power, M.: The Audit Society: Rituals of Verification, New edition, 208 p. Oxford University Press, Oxford (1999)
17. Weber, M.: Wirtschaft und Gesellschaft, 868 p. Mohr, Tübingen (1922)
18. Hutter, B.: Anticipating Risks and Organising Risk Regulation, 320 p. Cambridge University Press, Cambridge (2010)
19. Beck, U.: Living in the world risk society: a Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics. Econ. Soc. **35**(3), 329–345 (2006)
20. Schneier, B.: Beyond Fear: Thinking Sensibly About Security in an Uncertain World, 2nd edn., 296 p. Copernicus, New York (2003)
21. Cofta, P., Furnell, S.: Understanding Public Perceptions: Trust and Engagement in ICT-mediated Services, 262 p. International Engineering Consortium, Chicago (2008)
22. Schneier, B.: Liars and Outliers: Enabling the Trust that Society Needs to Thrive, 366 p. Wiley, Indianapolis (2012)
23. Luhmann, N.: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 140 p. Lucius & Lucius, Stuttgart (2000)
24. Ostrom, E.: Towards a behavioral theory linking trust, reciprocity and reputation. In: Ostrom, E. (ed.) Trust and Reciprocity, pp. 19–79. Oxford University Press, New York (2003)
25. Hamill, H., Gambetta, D.: Streetwise: How Taxi Drivers Establish Customers' Trustworthiness, 256 p. Russell Sage, London (2005)
26. Simmel, G.: Soziologie. Untersuchungen über die Formen der Vergesellschaftung, 804 p. Duncker and Humblot, Leipzig (1908)
27. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edn., 1080 p. Wiley, New York (2008)
28. Gambetta, D.: Signalling. In: Hedström, P., Bearman, P. (eds.) The Oxford Handbook of Analytical Sociology, pp. 168–194. Oxford University Press, Oxford (2009)
29. Beck, U.: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Suhrkamp, Frankfurt (1986)

30. Giddens, A.: The Consequences of Modernity, New edition, 200 p. Polity Press, Cambridge (1991)
31. Ostrom, E.: Trust and Reciprocity, 409 p. Oxford University Press, New York (2003)
32. Goldthorpe, J.: On Sociology: Numbers, Narratives, and the Integration of Research and Theory, 337 p. Oxford University Press, Oxford (2000)
33. Weesie, J., Buskens, V., Raub, W.: The management of trust relations via institutional and structural embeddedness. In: Doreian, P., Fararo, T.J. (eds.) The Problem of Solidarity: Theories and Models. Taylor & Francis, Boca Raton (1998)
34. Arksey, H., Knight, P.: Interviewing for Social Scientists, 224 p. Sage Publications Ltd., London (1999)
35. King, G., Keohane, R., Verba, S.: Designing Social Inquiry: Scientific Inference in Qualitative Research, 300 p. Princeton University Press, Princeton (1994)
36. Corbin, J.M., Strauss, A.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, 3rd edn., 400 p. Sage, Los Angeles (2008)
37. Silverman, D.: Doing Qualitative Research, 3rd edn., 472 p. Sage, London (2009)
38. Miles, M., Huberman, M., Saldana, J.: Qualitative Data Analysis - A Methods Sourcebook. Sage, London (2014)
39. Spence, M.: Job market signaling. Q. J. Econ. **87**(3), 355–374 (1973)
40. Spence, M.: Signaling in retrospect and the informational structure of markets. Am. Econ. Rev. **92**(3), 434–459 (2002)
41. Battigalli, P.: Rationalization in signaling games: theory and applications. Int. Game Theory Rev. **8**(1), 67–93 (2006)
42. Jonsson, J.O.: Explaining sex differences in educational choice an empirical assessment of a rational choice model. Eur. Sociol. Rev. **15**(4), 391–404 (1999)
43. McPherson, M., Smith-Lovin, L., Cook, J.M.: Birds of a feather: homophily in social networks. Ann. Rev. Sociol. **27**, 415–444 (2001)