To be published in Computer Fraud & Security (2016). https://doi.org/10.1016/S1361-3723(16)30091-4

INSIDER THREAT RESPONSE AND RECOVERY STRATEGIES OF FINANCIAL SERVICES FIRMS

Jacqueline Eggenschwiler, Ioannis Agrafiotis, and Jason R.C. Nurse
Department of Computer Science, University of Oxford, UK

Short abstract: This article analyses how financial services institutions address the threat from insiders, and in particular, how they respond to and recover from damaging insider-threat incidents.

Long abstract: Insiders have become some of the most widely cited culprits of cybercrime. Over the past decade, the scale of attacks carried out by insiders has steadily increased. Financial services firms, in particular, have been frequent targets of insider attacks. While insider-threat awareness levels have grown over the years, threat management strategies remain to be better understood. This article analyses how financial services institutions address insider threat, and how they respond to, and recover from insider-threat incidents. It is argued that response and recovery strategies of financial services organisations are still nascent. Combining industry reports, academic literature, and semi-structured interviews with senior financial services security professionals, the research offers a practice-oriented perspective on insider-threat response and recovery strategies, and identifies best practices.

INTRODUCTION

Over the past decade, the number and scale of attacks carried out by insiders has seen a steady increase. [1] Financial services firms, in particular, have been frequent targets of insider attacks. [2]

Historically, information security efforts of financial services firms have centred on defending external borders from intrusion by nefarious outsiders. More recently however, security debates have broadened to include trusted employees, contractors, and business partners. [3] Financial services institutions have grown increasingly aware of the changing threat landscape and the debilitating effects of insider attacks on the confidentiality, integrity, and availability of financial data and systems. [4]

While insider threat awareness levels have increased over the years, insider threat management practices remain to be better understood. Little is known about the spectrum of measures taken by financial services firms in response to insider attacks. In an attempt to acquire a better and more comprehensive understanding of insider threat response and recovery practices, the article seeks to address the following questions: How do financial services firms tackle insider threat? How do they respond to insider threat incidents? And what means of recovery do they employ?

For the purpose of this article, insiders are defined as current or former employees, contractors, or business partners who have or had authorised access to an organisation's network, system, or data and have exceeded or used that access, intentionally or unintentionally, in a manner that adversely affected the confidentiality, integrity, or availability of the organisation's network, system, or data. [5]

Combining industry reports, academic literature, and semi-structured interviews with senior financial services security professionals, this article moves away from a purely theoretical investigation, and pays due regard to the practical realities of insider threat management.

The remainder of this article is organised along four sections. The first section reviews relevant background literature on insider threat management. The second section provides a short industry overview and outlines the research aim and methodology of the article. The third section presents and discusses the findings obtained from industry reports, semi-structured expert interviews, and secondary literature research, and highlights best practices. The fourth section summarises the results.

RELATED WORK

Insider threat has advanced to an issue of growing concern and significance, a fact also reflected in the soaring number of publications dedicated to the topic. [6] Contributions cover a wider range of different themes spanning from behavioural research to technical attack modelling. [7–10]

Insider threat management denotes an emerging focus area of operational risk and information security management. It is concerned with addressing the security threats posed to organisations by trusted individuals who have intricate

knowledge of internal operations and processes, and/or access to sensitive systems and data. [11] The key building blocks of effective insider threat management mirror those expressed in the NIST Framework for Improving Critical Infrastructure Cybersecurity, and include: identify, protect, detect, respond, and recover. [12]

The framework allows organisations to individually assess threats most relevant to their operations "and to develop a risk-based approach to resource allocation". [13] It enables organisations to express their insider threat management efforts in terms of critical assets (*identify*), implemented controls and safeguards (*protect*), manifested threats (*detect*), formulated incident response strategies (*respond*), and business continuity plans (*recover*).

Much of the research on insider threat management has focused on pre-emptive protection and detection strategies. Sasaki, for example, promotes a detection framework based on psychological triggers that impels insiders to behave suspiciously. [14] Legg et al advocate a tiered insider threat detection model that incorporates elements from enterprise, people, technology, information, and physical domains. [15] Nurse et al introduced a framework for characterising, and later, detecting insider attacks, based on technical, psychological and behavioural factors. [16] And Hashem et al advance an insider threat monitoring and detection framework based on human bio-signals (electroencephalography and electrocardiogram signals). [17]

In contrast, response and recovery tactics have received less scholarly attention. However, the continuous surge in the number of insider threat incidents warrants closer examination of organisational response and recovery strategies. [18–20] Neither protection nor detection schemes offer absolute security. Trusted insiders often have intimate knowledge about the controls and detection mechanisms in place and are able to side-step existing physical and electronic security measures by legitimate means. No single prevention or detection framework can guarantee total security, which is why adequate response and recovery strategies are all the more important. Trzeciak holds: "It is essential that organisations […] take the necessary steps to ensure organisational resilience by implementing and regularly testing [response] and recovery processes". [21]

According to research conducted by the National Cybersecurity Institute, incident response is a complex undertaking, involving a wide range of organisational departments. Insider threat incidents are motivated by a combination of tech-

nical, behavioural, and organisational factors. As a result, effective management requires a disciplined, risk-based, cross-functional, approach that includes corporate security, Information Technology (IT), information security, legal, Human Resources (HR), audit, and other relevant control functions.

Insider threat response and recovery strategies are of critical importance to an organisation's overall security posture. They are key constituents of successful insider threat management, and worthy of more comprehensive analysis.

CONTEXT, RESEARCH AIM, AND METHODOLOGY

The main objective of this article is to examine the insider threat response and recovery practices of financial services firms. The research questions at the centre of interest are:

- How do financial services firms tackle insider threat?
- How do they respond to insider threat incidents?
- And what means of recovery do they employ?

Financial services firms are organisations that conduct financial transactions such as investments, loans or deposits, and devise and sell financial products. There exist various types of financial services firms, including banks, insurance companies, asset management boutiques, credit card companies, consumer finance enterprises, stock brokerages, investment funds, and government sponsored entities. [22]

As custodians of highly sensitive data and valuable physical assets, financial services institutions represent prime targets of information attack. According to research conducted by Websense Security Labs, financial services firms are under constant barrage by cybercriminals. "On average, financial services businesses are attacked 300 percent more than other [institutions]". [23] Attacks carried out by internal miscreants rank among the most pressing information security challenges of financial services firms. Cases such as Morgan Stanley, underline the severity of insider threat for financial services firms.

In order to acquire a better and more comprehensive understanding of the insider threat response and recovery strategies of financial services firms, the article employs qualitative means of data collection and analysis. Qualitative methods subsume a broad collection of naturalistic, interpretative approaches, focused on exploring phenomena from the inside. Qualitative methods describe a

"set of interpretive, material practices that make the world visible. These practices transform the world. They turn the world into a series of representations, including field notes, interviews, conversations [...]". [24] They are particularly suitable for scholarly ventures aiming to obtain a better understanding and sense of real world complexities and intricate social phenomena.

Methodologically, the article draws on a number of different sources, including secondary academic literature on insider threat management, primary materials on industry developments, as well as semi-structured interviews with senior financial services security professionals.

A total of five semi-structured interviews were conducted with senior financial services security professionals. Interviews were given some structure using an interview guide. Research participants were selected on the basis of their exposure to the financial services industry as well as their expertise in the area of information security management. Participants were primarily recruited via email and social media (LinkedIn) and came from backgrounds including banking, asset management, and consumer credit. The majority of interviewees benefited from international experience and global exposure. For reasons of confidentiality, names and corporate affiliations will not be disclosed. Relevant opinions voiced by the interviewees will be referenced indirectly.

In addition to semi-structured interviews, data was collected by means of online desk research. Databases queried included, among others, IEEE Xplore, EBSCOhost, ACM Digital Library, Google Scholar, Google Books, as well as Search Oxford Libraries Online (SOLO). The key search terms encompassed *insider threat management practices*, *insider threat response and recovery strategies of financial services firms*, *incident response measures of financial services firms*, as well as *insider threat management cycle*.

Patterns/themes within the data collected were identified, analysed, and reported with help of thematic analysis. Thematic analysis is a research technique that "minimally organises and describes [data sets] in rich detail". [25]

FINDINGS AND DISCUSSION

This section reports and discusses the theoretical and empirical results of the study. The findings are organised along the research questions outlined earlier.

How do financial services firms tackle insider threat?

Incidents of fraud, theft, and abuse, emanating from internal miscreants, present financial services firms with serious challenges. Launched with intricate knowledge of internal processes and procedures, "such threats have the ability to create sizable risks in relation to digital assets and are also the most challenging to manage". [26]

Empirical evidence confirms the prevalence of insider threat across financial services enterprises. With the exception of one interviewee, participants confirmed that their respective organisations have been subject to insider attacks. In line with industry accounts, participants reported that the majority of insider attacks are based on financial motivations and frequently involve data theft. Other motives exist, eg revenge, disgruntlement, or corporate espionage, but are less prevalent.

Participants mentioned that security breaches emanate from all types of roles and responsibilities. They further stated that the handling of insider incidents is highly complex and challenging. Effective insider threat management usually involves a great number of different stakeholders, and is often done behind closed doors so as to avoid negative publicity and reputational damage.

The fact that the majority of insider threat cases are dealt with internally and go unreported, limits the positive effects of data sharing and leaves industry partners "vulnerable to risks because those that hire these individuals in the future have no way to assess their threat potential". [27]

Rather than constituting a separate policy domain, respondents confirmed that insider threat is generally addressed in the context of wider risk management. With the exception of one financial services organisation, none of the firms surveyed had stand-alone insider threat handling policies in place. Given the severity of the risk, however, dedicated insider threat policies would help embed the issue more firmly and permanently. Policy commitment and adherence are absolutely critical for addressing insider breaches in a systematic and robust manner.

Respondents highlighted that effective mitigation and containment of insider attacks require the presence of tried and tested incident response plans. These plans have to come into effect immediately after detection, and follow clear execution guidelines. Pre-incident simulation exercises as well as senior management buy-in are vital for successful execution. Senior management support is important for two reasons: For one thing, "company executives understand the

negative effects of malicious insiders and support corrective actions, [for another, employees know] that senior leadership fully [back] insider threat efforts and a prompt response to illegal activities". [28]

Effective, expeditious, and judicious execution of incident response plans is particularly challenging across matrix organisations, where responsibilities overlap at times and accountabilities are not always well-defined.

Misalignment between key response functions can negatively affect organisations, both financially and organisationally. Consequently, clear, policy-driven governance structures are essential for successful insider threat management.

Successful response plans "take an interdisciplinary approach involving a combination of technology, legal, policy, physical security, awareness […], and counter intelligence resources. Incident response plans commonly revolve around the following core activities:

- Initial incident assessment (following detection)
- Cross-functional communication of attack
- Damage control and risk minimisation
- Detailed severity assessment
- Forensic analysis and evidence protection
- Notification of third parties where applicable

"These steps are not purely sequential. [Rather, they should happen alongside each other or throughout the incident]. For example, documentation [should] start at the very beginning and continue throughout the entire life cycle of the incident; communication, too, [should] happen throughout the entire incident".

The majority of respondents corroborated that incident response activities demand a high degree of departmental collaboration and that their respective organisations employ cross-functional computer security incident response teams to address insider attacks. Insider threat management has to be regarded as a critical organisational function that develops over time, not as a temporally limited project. [29] As a result, it requires continuous participation and commitment from a wide variety of stakeholders. "It also [demands] participation from appropriate lines of business, as well as finely tuned data privacy policies".

How do financial services firms respond to insider threat incidents?

Insider threat response measures can take many different forms, but can broadly be divided into two categories: internal and external measures.

External insider threat response measures denote a collection of response activities that are conducted in cooperation with company-external third parties, eg law enforcement agencies. In contrast, internal insider threat response measures describe a set of enterprise-specific remediation options that are executed without the involvement of third parties. Re-training efforts and organisational sanctions are but two examples of internal incident response measures.

Depending on the motivation, severity, and scale of insider attacks, internal response measures are preferred over external ones. According to the senior financial services security professionals interviewed, insider incidents are only reported to external bodies, eg national reporting entities, CERTs, or law enforcement agencies, in case of egregious breaches, ie where intent, severity, and scale warrant civil or criminal prosecution.

Considering recent regulatory developments, this kind of reporting behaviour might (need to) change in the near future. On 6 July 2016, the European Parliament and the Council adopted a directive that requires operators of essential services, including financial services firms, to "notify without undue delay the competent authority or the [national] Computer Security Incident Response Team (CSIRT) of incidents having a significant impact on the continuity of essential services they provide". [30] The Directive on security of network and information systems (NIS Directive) has yet to be implemented but could potentially have far-reaching effects on the incident reporting behaviour of financial services firms, requiring them to report more frequently and more transparently.

When carrying out legal actions, financial services firms are well-advised to coordinate response procedures with relevant other departments, especially General Counsel, and consider privacy and civil liberties at all times. [31]

Legal prosecution requires the production of clear and convincing evidence, eg by use of forensic analysis. The burden of proof lies with the attacked financial services organisation.

According to the experts interviewed, many financial services firms abstain from involving law enforcement agencies or legal charges because doing so:

- Involves a great amount of red tape (high administrative burden and agency cost) and creates a public record;

- Can cause irreparable reputational damage (loss of brand image);
- Has the potential to severely weaken a company's competitive position (loss of market share);
- Increases liability exposure.

Although, from a corporate/strategic perspective, a certain level of reluctance to involve third parties might be justifiable, engaging with law enforcement agencies can yield certain benefits. First of all, it can help recover damages and protect (intellectual) property, and second of all, it can help prevent other organisations from hiring charged internal miscreants in the future.

Financial services firms should consider the full spectrum of disciplinary options, including legal measures, when responding to insider threat incidents. Merely dismissing insiders defers a potentially dangerous problem to another unsuspecting enterprise. [32] At the same time, pursuing an approach that is too heavy-handed can create pitfalls for financial services firms where none used to exist. It can, for example, lead to indiscreet inquiries, unsubstantiated allegations, and accusations that negatively affect employee morale and corporate culture. "Users tied up in complex and over-controlling systems are unable to perform. Too light a touch sees key assets and resources too easy to misuse, alter, or steal".

Financial services firms have to strike a fine balance between lightweight disciplinary measures and punitive sanctions, and between protection, control, and value creation, respectively.

What means of recovery do financial services firms employ?

Successful insider threat management involves incident recovery, ie restoration of the confidentiality, integrity, and availability of affected systems and data. [33] Incident recovery is as complex as incident response and involves the following core activities:

- Recovery of systems and data
- Compilation and organisation of incident documentation
- Assessment of incident damage and cost
- Review of response measures and issuance of policy updates where applicable
- Roll-out of staff trainings and education

In line with secondary research, respondents confirmed that incident review and integration of response learnings are key success factors for effective recovery. [34] Insider threat recovery requires the cooperation of an entire organisation, not just the technical departments and security functions. Reducing follow-up activities to IT and security departments runs the risk of excluding other corporate functions that also play a crucial role in incident recovery, and inhibits organisational learning.

Lessons learned have to be incorporated into company-wide incident response plans, and have to be communicated to wider staff accordingly. This allows employees to get acquainted with organisational insider threat response measures and helps them understand that insider threat incidents are taken seriously.

On the topic of communication, senior financial services security professionals stated that informal communication and exchange of threat intelligence among peers is invaluable for successful recovery. The question arises, whether collaboration would yield even more benefits if it were institutionalised more formally. More institutionalised communication and exchange of security intelligence would, for example, aid the dissemination of industry best practices for insider threat response and recovery.

According to the experts interviewed, educational measures, such as employee trainings or awareness campaigns, also play a vital role for successful insider threat recovery. Financial services firms have addressed the need for educational measures with a number of different training instruments, including compulsory in-person training sessions, web-based online class-rooms, as well as video-based information campaigns.

While the existence of relevant training instruments is essential, they do not represent a carte blanche for effective recovery. Training instruments have to be assessed for their effectiveness on a regular basis, and educational measures adjusted and updated where necessary. Financial services firms must ensure that their employees are presented with relevant, up-to-date, and engaging learning content. Relevant employee education is a key contributor to enhanced organisational resilience, and indispensable for effective insider threat management.

Meaningful and enduring recovery cannot be achieved effectively without the buy-in of senior management. Among other things, top-down support helps im-

prove regulatory compliance and ensures "that appropriate safeguards are in place to mitigate legal action that may result from an internal breach".

In order to further strengthen and mature their insider threat response and recovery strategies, financial services firms should consider the following best practices:

- Establish clear insider threat management governance structures
- Devise, implement, follow, and periodically review dedicated insider threat management policies
- Coordinate, memorise, and streamline response and recovery measures and consider employing relevant third parties, eg law enforcement agencies, more frequently
- Ensure transparent communication of response and recovery measures to relevant stakeholders and create a sense of ownership among them
- Formalise threat intelligence sharing activities and leverage key learnings across organisations
- Provide staff with relevant insider threat education and development programmes, and ensure regular reviews of programme effectiveness
- Evaluate response and recovery practices and include lessons learned into future activities
- Ensure senior management buy-in and award the right level of attention to insider threat management

CONCLUSION

Financial services firms represent some of the most highly regulated and protected entities of the private sector. At the same time, they represent perennially attractive targets for cyberattacks. According to primary as well as secondary research, financial services firms are under more scrutiny than ever for the security of their critical assets (tangible and intangible). Rogue insiders in particular, present these enterprises with serious challenges. Although financial services organisations have grown increasingly aware of the shifting threat landscape and the debilitating effects of insider attacks on the confidentiality, integrity, and availability of financial data and systems, insider threat response and recovery strategies are still nascent.

Results obtained from industry reports, academic literature, and semi-structured interviews suggest that effective, organisationally-entrenched, insid-

er threat management practices continue to be a work in progress for many financial services firms. Comprehensive insider threat management policies are largely absent, and incident response measures often too light-touch, leaving financial services firms, their data, and systems exposed and vulnerable.

While insider threat management programs cannot not guarantee absolute protection, well thought-out response and recovery strategies can equip financial services firms with the necessary means to counter internal risks more effectively and rehabilitate from incidents more quickly, capabilities that contribute to enhanced organisational resilience.

Given the prevalence and potentially far-reaching consequences of insider threat incidents, financial services firms need to recognise insider threat management as an obligation that can no longer be ignored, and a function that requires corresponding organisational attention.

BIBLIOGRAPHY

1 PricewaterhouseCoopers. 'Managing insider threats'. PwC, 2015. Accessed Aug 2016. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/managing-insider-threats.html.

2 Vormetric. '2015 Vormetric Insider Threat Report'. Vormetric, 2015. Accessed Aug 2016. https://www.vormetric.com/campaigns/insiderthreat/2015/.

3 Wall, David. 'Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders'. Symantec, 2011. Accessed Aug 2016. http://www.symantec.com/content/de/de/about/downloads/press/WP_Organizational_Security_and_the_InsiderThreat_Malicious_Negligent_and_Well-Meaning_FINAL.pdf.

4 Hardy, Mark. 'Risk, Loss and Security Spending in the Financial Sector: A SANS Survey'. SANS Institute InfoSec Reading Room, 2014. Accessed Aug 2016. https://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690.

5 Silowash, George; Shimeall, Timothy; Cappelli, Dawn; Moore, Andrew; et al. 'Common Sense Guide to Mitigating Threats'. Carnegie Mellon University, 2012. Accessed Aug 2016. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf.

6 Nurse, Jason R C; Legg, Philip: Buckley, Oliver: Agrafiotis, Ioannis; et al. 'A critical reflection on the threat from human insiders - Its nature, industry perceptions, and detection approaches'. Lecture Notes in Computer Science, Vol. 8533, 2014, pp. 270–281. http://link.springer.com/chapter/10.1007%2F978-3-319-07620-1_24.

7 Randazzo, Marisa; Keeney, Michelle; Kowalski, Eileen; Cappelli, Dawn; Moore, Andrew. 'Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector'. Carnegie Mellon University, 2005. Accessed Aug 2016. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50287.

8 Ha, Duc; Upadhyaya, Shambhu; Ngo, Hung; Pramanik, Suranjan; et al. 'Insider threat analysis using information-centric modeling'. IFIP International Conference on Digital Forensics, Vol. 242, 2007, pp. 55–73. http://link.springer.com/chapter/10.1007%2F978-0-387-73742-3_4.

9 Martinez-Moyano, Ignacio J; Rich, Eliot; Conrad, Stephen; Andersen, David F; Stewart, Thomas R. 'A behavioral theory of insider-threat risks: A system dynamics approach'. ACM Transactions on Modeling and Computer Simulation (TOMACS), 2008, Vol. 18, pp. 7–27. https://ai2-s2-

pdfs.s3.amazonaws.com/3e7a/be770186c0b74cb70fc7f036ae3625e86218.pdf.

10 Khader, Majeed. 'Combating Violent Extremism and Radicalization in the Digital Era'. IGI Global, 2016.

11 Steele, Sean; Wargo, Chris. 'An Introduction to Insider Threat Management'. Information Systems Security, Vol. 16, 2007, pp. 23–33. http://www.tandfonline.com/doi/abs/10.1080/10658980601051334?journalCode=uiss19.

12 National Institute of Standards and Technology. 'Framework for Improving Critical Infrastructure Cybersecurity'. National Institute of Standards and Technology, 2014. Accessed Aug 2016. http://www.cslawreport.com/files/2015/04/07/nist-combined-file.pdf.

13 Securities Industry and Financial Markets Association. 'Insider Threats Best Practices'. Securities Industry and Financial Markets Association, 2014. Accessed Aug 2016. https://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/sifma-cybersecurity-insider-threat-best-practices.pdf?n=26416.

14 Kundisch, Dennis. 'New Strategies for Financial Services Firms: The Life-Cycle-Solution Approach', Physica-Verlag, 2003.

15 Legg, Philip; Moffat, Nick; Nurse, Jason R C; Happa, Jassim; et al. "Towards a conceptual model and reasoning structure for insider threat detection". Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 4, 2013, pp. 20-37. http://www.scopus.com/inward/record.url?eid=2-s2.0-84890952452&partnerID=tZOtx3y1.

16 Nurse, Jason R C; Buckley Oliver; Legg Philip; Goldsmith Michael; et al. "Understanding insider threat: A framework for characterising attacks". IEEE Security and Privacy Workshops (SPW), 2014, pp. 214-228. IEEE. http://ieeexplore.ieee.org/document/6957307/?arnumber=6957307

17 Hashem, Yessir; Takabi, Hassan; Ghasemigol, Mohammad; Dantu, Ram. 'Inside the Mind of the Insider: Towards Insider Threat Detection Using Psychophysiological Signals'. Journal of Internet Services and Information Security, Vol. 6, 2016, pp. 20–36. http://isyou.info/jisis/vol6/no1/jisis-2016-vol6-no1-02.pdf.

18 Sullivant, John. 'Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency'. Butterworth-Heinemann, 2016.

19 Davis, John S; Libicki, Martin C; Johnson, Stuart E; Kumar, Jason; et al. 'A Framework for Programming and Budgeting for Cybersecurity'. RAND, 2016. Accessed Aug 2016. http://www.rand.org/pubs/tools/TL186.html.

20 EY. 'Managing insider threat'. EY, 2016. Accessed Aug 2016. http://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf.

21 Trzeciak, Randy. 'Common Sense Guide to Mitigating Insider Threats'. Carnegie Mellon University, 2013. Accessed Aug 2016. https://insights.sei.cmu.edu/insider-threat/2013/02/common-sense-guide-to-mitigating-insider-threats---best-practice-15-of-19.html.

22 Singh, Parmvir. 'The role of Banking and Financial Services industry in economic recovery'. Online International Interdisciplinary Research Journal, Vol. 5, 2015, pp. 187–193. http://www.oiirj.org/oiirj/nov2015-special-issue/22.pdf.

23 Websense Security Labs. '2015 Industry Drill-Down Report'. Forcepoint, 2015. Accessed Aug 2016. https://www.forcepoint.com/thank-you-your-interest-whitepaper?first_name=&last_name=&email=&form_id=1363&file=2726&resource=4041.

24 Denzin, Norman K; Lincoln, Yvonna S. 'The SAGE Handbook of Qualitative Research'. SAGE, 2011.

25 Braun, Virginia; Clarke, Victoria. 'Using thematic analysis in psychology'. Qualitative Research in Psychology, Vol. 3, 2008, pp. 77–101. http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.

26 Heindl-Schober, Angela. 'Insider Threats: Spotting the Inside Job'. Vectra Networks, 2014. Accessed Aug 2016. http://blog.vectranetworks.com/blog/topic/insider-threats.

27 PricewaterhouseCoopers. 'Managing cyber risks in an interconnected world'. PwC, 2015. Accessed Aug 2016. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

28 TechNet. 'Responding to IT Security Incidents'. Microsoft, 2016. Accessed Aug 2016. https://technet.microsoft.com/en-us/library/cc700825.aspx.

29 Solomon, Dan. 'Why collaboration is the only way to combat cyber threats'. ComputerWeekly.com, 2014. Accessed Aug 2016. http://www.computerweekly.com/opinion/Why-collaboration-is-the-only-way-to-combat-cyber-threats.

30 European Parliament and Council of the European Union. 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union'. Official Journal of the European

Union, Vol. 194, 2016, pp. 1-30. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

31 Huth, Carly; Ruefle, Robin. 'Components and Considerations in Building an Insider Threat Program'. Carnegie Mellon University, 2013. Accessed Aug 2016. https://resources.sei.cmu.edu/asset_files/Webinar/2013_018_101_69083.pdf.

32 Intelligence and National Security Alliance. 'A preliminary examination of insider threat programs in the US private sector'. Intelligence and National Security Alliance, 2013. Accessed Aug 2016. http://csrc.nist.gov/cyberframework/framework_comments/20131213_charles_alsup_insa_part4.pdf.

33 Torres, Alissa. 'Incident Response: How to Fight Back'. SANS Institute InfoSec Reading Room, 2014. Accessed Aug 2016. https://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342.

34 Francis, Ryan. '9 steps for a successful incident response plan'. CSO Online, 2016. Accessed Aug 2016. http://www.csoonline.com/article/3099684/disaster-recovery/9-steps-for-a-successful-incident-response-plan.html#slide10.

ABOUT THE AUTHORS

Jacqueline Eggenschwiler is a researcher at the University of Oxford's Centre for Doctoral Training in Cyber Security. Her research interests include insider threat, cybercrime, and internet governance. Jacqueline holds degrees in International Affairs and Governance, International Management, and Human Rights from the University of St. Gallen and the London School of Economics and Political Science.

Ioannis Agrafiotis is a Research Fellow (Senior Researcher) in the Department of Computer Science at the University of Oxford, where he currently explores novel ways to capture organisational cyber harm and risk. Ioannis is also working on a project aiming at detecting insider threats. His research interests include automated network defence and business process modelling, information trustworthiness, online privacy and dynamic consent, insider threat, and anomaly detection.

Jason R.C. Nurse is a Research Fellow (Senior Researcher) in the Department of Computer Science at the University of Oxford. He has worked within industry and academia throughout his career. This has included several IT positions within industry, and academic posts such as Research Fellow at Warwick University, and more recently, his role at Oxford. Jason has published several articles at both journal and conference levels and also sits on the programme committee of related venues. His research interests include insider threat, information security and trust, investigating the risks to identity security and privacy online, mobile device security, human factors of security and insider threats.