• Utilising their data to reach new customers rather than focusing solely on avoiding data breaches.

**Effective management**

Information governance, a multi-disciplinary framework that businesses can employ to encourage appropriate action and behaviour with regard to how information is valued, managed and used by the organisation, may seem like a daunting concept for businesses of all sizes and areas of operation but its principles sit at the heart of a practical and effective approach to information risk management.

Information governance is about understanding what information you hold, where you hold it and what its value is — to you, your employees, your customers and your competitors — how it moves through the business and where it is most vulnerable. It’s about making sure information management and risk are on the board agenda and are backed by empowered and suitably resourced multi-functional teams.

It is clear from the research that, while many organisations have developed policies and may have emerging governance capabilities, there has been insufficient action in the business to drive the necessary risk assessments and controls design and monitoring that is needed for effective information governance.

While this article has focused on risks, it is important to remember that, in defining requirements, management have the opportunity to use governance to drive improvement and to identify information needs for the future. Questions need to be asked to enable organisations to do what they can’t do now and seize the opportunities in the digital economy — for example, ‘if we had this information, could we make that strategic decision?’ This is the upside of governance.

Engage with key business stakeholders in developing an information management strategy that can support growth and promote an open/sharing culture while maintaining a level of protection over important information assets. Security of information is key within any organisation, but alongside mitigating risks, it’s imperative to ensure that value is derived from the information at hand.

**About the author**

Sue Trombley is managing director of professional services at Iron Mountain, and has more than 25 years of information governance consulting experience. Prior to her current role, Trombley led Iron Mountain’s consulting group responsible for business development, managing a team of subject matter experts and running large engagements. Trombley holds a master’s degree in Library and Information Science and is an ARMA-certified Information Governance Professional. She sits on the AIIM International Board, the University of Texas at Austin School of Information Advisory Council, and is VP of the Boston ARMA chapter.

**References**

1. ‘Beyond Good Intentions: The need to move from intention to action to manage information risk’. PwC and Iron Mountain. www.ironmountain.co.uk/risk-management/-/media/bb998703a43e5de2b5d281e-de4eb15e0.pdf.

---

**Identifying attack patterns for insider threat detection**

Ioannis Agrafiotis, Jason RC Nurse, Oliver Buckley, Phil Legg, Sadie Creese, Michael Goldsmith

The threat that insiders pose to businesses, institutions and governmental organisations continues to be of serious concern. Recent industry surveys provide unequivocal evidence to support the significance of this threat and its prevalence in enterprises today. In an attempt to address this challenge, several approaches and systems have been proposed by practitioners and researchers. These focus on defining the insider threat and exploring the human and psychological factors involved, through to the detection and deterrence of these threats via technological and behavioural theories.

While these approaches are valuable, they often consider only specific parts of the problem to the detriment of the wider insider-threat problem space. In previous work therefore, we aimed to address this oversight by developing a unifying framework to fully characterise insider attacks. This included a clear definition of which insiders attack, why they attack, the human factors that lead to malicious and accidental threats, how an individual’s background may impact the likelihood of attack, what behaviour may be exhibited before or during an attack, what the common attack vectors and steps within an
attack are, and what assets and vulnerabilities are typically targeted.

Identifying patterns

In this article, we aim to extend that work and investigate the use of the framework in identifying attack patterns for insider-threat detection. Our goal is to then use such patterns within our machine learning-based threat-detection prototype. Using techniques such as machine learning to identify anomalies in employees’ behaviour is a demanding and onerous task. In order to provide effective solutions there is a need to establish a process that will aid in rationalising the results of potential anomaly metrics. Anomaly metrics are the results of detection systems that describe which attributes insiders exploit. We believe that attack patterns could be quite useful for this task, hence our aim in using the framework presented in our previous work for understanding insider-threat behaviour and defining these patterns.

More specifically, we expand the attack characteristics of our framework, by detailing attack steps that describe atomic activities in the attacks. For this we use 120 insider-threat case studies to create a chain of attack steps that culminate in the end-goal of the attacker (e.g., committing fraud). We then design attack-pattern trees comprising of the attack steps and highlight the most prevalent paths for every attack type. In addition, we establish how different attack steps relate to anomaly metrics derived from our existing detection approach. Towards this end, we consider two case studies to illustrate how attack-pattern trees can assist in identifying useful anomaly metrics, while also providing insight into how metrics could be combined to support an organisation’s information technology (IT) team in their decision-making on potential insider threats.

Attack framework

Our framework for characterising insider attacks was created out of the need for an enhanced approach by which the various components of the insider-threat problem could be easily understood, presented and reflected upon. This objective served to guide our research and scope the creation of the framework. To build the framework itself, we adopted a grounded theory approach. This consisted of first collecting and examining a dataset of 80 insider-threat cases from CMU-CERT, the UK’s CPNI and various news articles.10–17

Once we examined these cases, we set about identifying key aspects of the insider attacks relating to the attackers, their background, their behaviours, and the attacks they conducted. The culmination of our analysis was a framework where we clearly defined how each of the key aspects relate to each other and the general progression of an insider attack. Generally, our framework consists of several classes of component pertaining to insider threat, and depicted in four areas. These areas are:

- **Attack catalyst** – containing a precipitating event.
- **Insider-threat characteristics** – detailing the individual’s personality characteristics, historical behaviour, psychological state, attitudes towards work, skill set, opportunity and motivation to attack.
- **Attack characteristics** – covering attacks, attack objectives, specific attack steps and attack step goals.
- **Organisation characteristics** – which specify the enterprise’s assets and vulnerabilities.

For further detail on the framework, readers are directed to our previous article.

Identifying attack patterns

As previously mentioned, this article aims to expand our research on the framework for characterising insider attacks, by focusing on insider attack patterns. Identifying attack patterns can be extremely helpful, as these patterns can provide the mechanism for combining different features and anomaly metrics, and set the context for understanding anomalous insider behaviour.

While attacks in our framework aim to be generic, ‘attack steps’ define, in detail, the specific activities undertaken to conduct the attack. As such, an attack can be composed of several chained steps. To steal sensitive IP, an insider threat may:

1. Determine which of their colleagues has the credentials to access the desired IP (reconnaissance).
2. Coerce those individuals possibly via financial means, charm or physical threats to assist in the task.
3. Use the ill-gotten credentials to access the IP.
4. Download the IP to portable media.
5. Delete the related log files.

These attack steps can also be thought of in terms of the value gained from each step, namely, the ‘attack step goal’. Thus, for the steps above, we would have:

2. Recruiting accomplices.
3. Accessing restricted data.
4. Exfiltration of a volume of data.
5. Covering tracks.

We believe that these goals can be particularly helpful when discussing the insider-threat problem with top management, and effectively communicating the attack, inclusive of what would be gained through each step, without going into excessive technical detail.

**Figure 1** shows an example sequence of attack steps within an attack, and highlights the strong sense of ordering within the attack. All steps at the same level in an attack tree are essentially in parallel, and so do not preserve any ordering. **Figure 1** highlights an idea of concurrency in our attack steps, as the initial stage of the attack sees the actor both developing a relationship with a rival company while at the same time gathering company secrets and IP in tandem. This example of attack steps can then be followed through, sequentially, to the IP being copied and finally the actor editing and deleting log files in order to hide the evidence of their attack.
De-constructing the case studies

Applying the grounded theory approach to derive the attack steps was an iterative process. Initially we assessed each one of the case studies and documented the emerging attack steps. The next task was to revisit the steps and group together those that had similar meaning. This process was repeated several times until we crystallised our interpretation of the attack-steps descriptions and no more reductions and groupings could be made. Due to limited space, we present the full spectrum of the attack steps identified in a supporting technical document available online.18

Attacks steps share some similarity with the pre-existing notion of ‘attack trees’, in that both methods can describe how a specific target or asset might be attacked.19 The value of our attack steps is that they allow for the clear sequencing and ordering of actions. The idea of ‘intrusion kill chains’ has particular relevance when considering our attack steps.20 These kill chains provide a means of describing the different phases of an intrusion and are modelled as a chain to emphasise the idea that if there is a breakdown at any one stage then the entire process is disrupted. Intrusion kill chains are designed to model attacks, with the aim of highlighting patterns within individual intrusions and how they may fit into part of a larger threat. It is easy to imagine how a similar aim could be achieved using our attack steps; when enough attacks have been collected and modelled then they could be used to establish common attack steps. The concept of building a library of attack steps is similar to the idea of Common Attack Pattern Enumeration and Classification (CAPEC).21 Attacks are recorded there in a similar fashion to our attack steps, and then CAPEC is used to identify opportunities for increasing the ‘robustness and defendability’ of software.

Developing attack patterns

Defining the attack steps was the first step towards identifying attack patterns; the next and most decisive was to reconstruct the case studies as a chain of attack steps. We studied all the case studies related to fraud and IP theft, and based on the narrative of each case study we developed the corresponding chain of attack steps. We then started forming attack patterns by following the attack tree paradigm.

“An employee who has no access to a database, will seek to upgrade his privileges before being able to download data, whereas an IT administrator with full access credentials will omit this step”

In an attack tree, its root comprises the end-goal of the attacker, the nodes represent intermediary steps to achieve the goal and the leaves of the trees are the initial steps of an attacker. Following this convention, we grouped together all the chains of case studies that ended with the same attack step. The final attack step was the root of our attack-pattern tree. We then placed all the steps prior to the final step in the root. For example, if an attack step was fourth in the chain of events of an attack in one case study and fifth in another, we would place the attack step in the fifth layer of the attack tree.

The depth of each attack-pattern tree is equal to the maximum length of the grouped case studies. The attacks, however, do not necessarily have to start at the same layer. This could be either due to lack of information from the case studies, where some omitted information pertaining to how the attack originated, or due to the different privileges and roles that the attackers have, rendering some of the steps irrelevant. For example an employee who has no access to a database, will seek to upgrade his privileges before being able to download data, whereas an IT administrator with full access credentials will omit this step.

The mismatch of layers where the attacks can begin motivated us to change the position of the nodes (the structure of the tree remained the same, we only moved the nodes to different layers) based on the description of the attack steps. Our aim was to categorise the layers of trees similarly to the intrusion kill chains stages. Attack steps describing related type of activity were placed in the same layer. We identified five different classes in which we categorised the layers of the attack-pattern trees, namely: normal behaviour; covering tracks; weaponisation; attack; and outcome. We further dichotomised attack steps to those that could potentially be observed automatically with the use of a software detection system, and to those that require human intervention. To illustrate this information, we coloured the attack steps that
can be detected by machines green and used red for the attack steps where human intervention is needed.

Figure 2 presents the attack-pattern tree where the aim of the attack is to misappropriate money from the insider’s employer by using electronic means. AS is for the attack step and the step number corresponds to the full set detailed in our supporting document. All the cases we analysed ended up in the attacker transferring company’s funds to personal accounts. There are eight different pathways depicted in the tree that attackers followed in the cases:

AS75; AS6; AS17; AS56; AS46; AS44
AS75; AS6; AS8; AS17; AS56; AS44
AS75; AS6; AS8; AS17; AS56; AS44
AS75; AS6; AS8; AS17; AS56; AS44
AS69; AS6; AS8; AS17; AS56; AS46; AS44
AS69; AS6; AS8; AS17; AS56; AS46; AS44
AS69; AS6; AS77; AS32; AS44
AS69; AS6; AS77; AS32; AS44

One of the longest paths (AS75; AS6; AS8; AS17; AS56; AS46; AS44) requires the attackers to use their credentials and obtain access to files that are within their privileges. In the following steps, insiders build a close relationship with employees who hold critical roles, in order to gain their trust and provide them with access to processes that they were not allowed to authorise. Then they would use the company’s systems to generate fake documentation, justifying the authorisation of these processes and create a new account to transfer the money from illegitimate claims.

The same attack can be executed by using credentials belonging to colleagues (AS69; AS6; AS9; AS17; AS56; AS46; AS44) in order for the insiders to cover their tracks. Shorter alternatives (AS75; AS6; AS8; AS17; AS56; AS44) and (AS75; AS6; AS77; AS56; AS44) omit steps that focus on concealing the tracks of the attack. The shortest path (AS75; AS6; AS77; AS56; AS44) or (AS69; AS6; AS77; AS32; AS44) can be achieved if the attackers have already clearance to authorise processes and file documentation for these claims, a fact that may imply a person with managerial role. Then they can either approve inappropriate transactions, as the AS56 step suggests, or fill in illegitimate claims for expenses. There are four cases where human intervention is required to determine whether attackers have used this step. These are AS8 where insiders build close relationships with other employees, AS17 where fake documentation is created, AS46 where unauthorised accounts are opened, or AS32 where illegitimate claims are filled in.

### Spectrum of attacks

Attack-pattern trees capture the spectrum of all the attacks described in the case studies. We endeavoured to identify trends in these attacks, by highlighting the most prevalent attack paths. For every attack-pattern tree we identify the most commonly followed path and we present the number of case studies in which this path occurred. In Figure 2, for example, the number next to the outcome step denotes that the prevalent path occurred in four out of eight case studies analysed.

In total, we have identified 19 different attack-pattern trees for cases related to fraud threats and one attack-pattern tree for cases related to IP thefts. We have made use of 44 different attack steps to design the attack-pattern trees and we have classified all the attack steps used as either machine detectable or those that require human intervention. Table 1

<table>
<thead>
<tr>
<th>Attack Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS9</td>
<td>Building a close relationship with company’s clients.</td>
</tr>
<tr>
<td>AS11</td>
<td>Coercing workers with access to company files to assist in an attack.</td>
</tr>
<tr>
<td>AS17</td>
<td>Creating fake documentation in general.</td>
</tr>
<tr>
<td>AS19</td>
<td>Creating fake receipts.</td>
</tr>
<tr>
<td>AS46</td>
<td>Opening illegitimate accounts using clients’ information.</td>
</tr>
<tr>
<td>AS53</td>
<td>Physical theft of files/computer systems/property belonging to company’s clients.</td>
</tr>
</tbody>
</table>

Table 1: Attack steps that would require some form of human intervention in order to be detected.
provides the list of the attack steps considered in this article that would require some form of human intervention for their detection. The attack steps that can be obtained by automated processes will be outlined in the next section. We will consider two case studies and provide details on how a detection system could capture the attack steps based on features derived from a user’s profile and anomaly metrics that relate deviations of observed features to suspected attack patterns. Due to space limitations, we illustrate only two attack-pattern trees. For diversity however, we present those comprised of the most attack steps.

Applying attack patterns for threat detection

Having defined the attack patterns observed in reported case studies of insider threats, here we show how attack steps could be identified through detection capabilities. In the prototype detection system that we have constructed as part of the Corporate Insider Threat Detection (CITD) project, we define a series of anomaly metrics. An anomaly metric indicates the amount of deviation that is currently being observed for a particular observation type. An observation type may exist for a particular activity – for instance, login anomaly or email anomaly – or for a particular type of observation that can be made, such as a new anomaly, or a role anomaly.

Detection system

By constructing user and role-based profiles, we can extract various features that define device and activity usage patterns, including hourly and daily usage frequency, new observations of activities and attributes across multiple devices, and new activities that do not exist within the profiles of their associated role. Our prototype detection system constructs anomalies based on each of the proposed metrics, by analysing the amount of deviation that is exhibited by features that relate to that particular anomaly type. The anomaly metrics that are used in the current detection prototype are:

1. Anomalies based on the how the user acts with respect to individual activities – login anomaly, login duration anomaly, logoff anomaly, USB insertion anomaly, USB duration anomaly, USB removal anomaly, email anomaly, web anomaly, file anomaly.
2. Anomalies based on how the user acts across different activities – this anomaly (observed on ‘this’ device), any anomaly (observed on ‘any’ device), new anomaly (triggered by a ‘new’ observation), hourly anomaly (triggered by a time-based observation), number anomaly (triggered by a count-based observation), user anomaly (triggered by a ‘user’ comparison), role anomaly (triggered by a ‘role’ comparison), total anomaly (observed over all observed features).

By considering the range of different anomalies that can occur on singular activities, and across multiple activities, this provides a means to relate anomaly alerts to a particular pattern of activity. For example, consider a user who scores highly on USB insertion anomaly, file anomaly, new anomaly, hourly anomaly, user anomaly, and role anomaly. Here, it could be established that the user has accessed files on the system that are new for this user, and inserted a USB storage device that again is new for the user, at an unusual time of the day, which differs significantly from how other users in the role are acting, and how this user has acted previously. Clearly, this is a user who should be flagged by the system, and the alert of different anomaly metrics allows the analyst to quickly establish not only that they have been flagged, but also why they have been flagged.

Having specified the different types of anomaly metrics that we currently cater for, we show how the proposed attack steps can be related to these anomaly metrics. In particular, we demonstrate how the attack steps related to the IP theft and fraud case studies can be captured by the proposed anomaly metrics.

IP theft case study

In the IP theft cases, the aim of the insider threat is to steal sensitive documents from their employers. The attack-pattern tree as illustrated in Figure 3 considers the six different approaches that insiders followed to achieve their goal. In this section’s case study we will illustrate how an anomaly-detection system can be configured based on information from the attack-patters trees to assist detection of IP theft.

Figure 3 presents the attack-pattern tree where the aim of the attack is IP theft. All the cases that were analysed resulted in the insider publishing/sharing sensitive company files to unauthorised parties. There are eight different pathways depicted in the tree that attackers followed in the these cases:

- A575; A56; A51; A577; A527; A558
- A575; A56; A527; A558
- A575; A56; A577; A558
- A575; A515; A576; A527; A558
- A575; A55; A527; A558
- A575; A56; A511; A527; A558
- A569; A57; A553; A558
- A575; A574; A57; A527; A558

The longest path (A575; A56; A511; A577; A527; A558) is for the attackers to log in using their credentials and obtain access to files that are within their privileges. The following step would require to coerce a colleague to provide them access to additional files that they are not allowed to obtain. Then they would use the company’s systems to download the files into a portable device, before sharing these with unauthorised third parties.

In certain cases, insiders decided to delete the files from companies’ systems after downloading them, suggesting an extra motivation for blackmail or sabotage (A575; A56; A511; A577; A527; A558). Shorter alternatives (A575; A515; A576; A527; A558) require the installation of a ‘back door’ in company’s systems to avoid logging in with their personal or their colleagues credentials.
The shortest path (AS75; AS6; AS27; AS58 or AS75; AS5; AS27; AS58) can be achieved if the attackers already have privileged access to these files, a fact that may imply a person with a managerial role. Then they can either access and browse normal volumes of files, as the AS6 step suggests or browse files that they do not usually visit.

There were cases where attackers, due to their roles, were able to produce fake access credentials and elevate their access credentials, before copying files (eg, AS75; AS6; AS11; AS27; AS22; AS58).

All of the aforementioned paths require the use of portable devices to exfiltrate the data from the company. There is, however, another attack where the insiders get possession of physical files, such as printouts. To achieve this, they access rooms using a colleagues’ credentials to obtain sensitive files stored there. It is worth noting that most of the attack steps could potentially be recognised by a detection system.

It is possible to reconfigure a detection system to cater for the attack steps described in this case study. All the attacks originate when employees log on to systems and access files legitimately. We do not expect an indicative anomalous metric for such actions except where employees log on to systems on irregular hours. In the case where they use their colleagues’ credentials, we expect to detect a new machine performing actions using the specific credentials. We may detect log-on from two different devices simultaneously from IP addresses that are in very different locations. In addition, the files accessed during the attack may be different to those accessed by people who hold the same role as the insiders, therefore we may have a file access anomaly if activities of the insider are compared to role activities.

“\textit{In some cases, insiders may choose to cover their tracks by deleting log files or sabotage the company’s systems by deleting sensitive files}”

The next level of the attack-pattern tree comprises attack steps where insiders use companies’ systems to download sensitive material to portable devices. In order to capture these steps, we need to consider data about files, activities on these files and insertion of portable devices. We expect a USB insertion anomaly, a USB duration anomaly and a USB removal anomaly to be flagged up in a detection system. In some cases, insiders may choose to cover their tracks by deleting log files or sabotage the company’s systems by deleting sensitive files. For these issues we should search for delete actions in data regarding files and an anomaly on file access and actions should be raised. In addition, to cater for cases where the insider may choose to install back-door software to acquire access to sensitive files, data from program installations, if available, should be considered and an anomaly on activities for machines should be identified.

The last step of the IP theft requires the attacker to publish or share the acquired sensitive files or information to unauthorised parties. Such actions may be detected by analysing data from activities and files for every machine. We expect file and activity anomalies for any device both per user and per role.

**Stealing clients’ money**

This case study considers how the attack-pattern trees can assist in detecting employees who defraud companies, specifically financial institutions such as banks, by transferring clients’ money to their personal accounts. Figure 4 illustrates all the possible pathways that an attacker may follow to conduct such an attack.

Initially, the attackers must log in to the system, either by using their credentials, or by using a remote access account. Anomalies may be detected either at unusual login hours that the attack may take place, or at the rare usage of remote access. In the case where insiders choose to use a colleague’s credentials, we expect to detect a new machine performing actions using the specific credentials for the first time.

The next level requires insiders to search and identify vulnerable clients (ie, elderly or very wealthy people who may not recognise funds missing). They will then start a series of illegitimate requests or transactions without the authorisation of the clients. In order to justify these actions they might choose to provide fake documentation, disrupt the services that these customers usually get from the organisations (ie, stop
receiving bank statements) and sometimes they will try to befriend them. At this stage we expect anomalies in the data about files that insiders search for. When compared to the data about files that their colleagues with similar roles search for, there should be an inconsistency. In addition, we expect unusual requests from clients that these insiders have searched for, and potential complaints of service disruption.

The final level comprises the illegitimate transaction of money from the clients’ accounts to the insiders’ account. Insiders may choose to cover their tracks by creating fake receipts to justify the transactions, by temporarily prohibiting their clients from accessing their accounts or by creating new fake accounts based on the clients’ information to which they have full rights.

Anomalies should be observed at the number of transactions that a client’s account will have towards a specific account and the number of new documents produced to justify these actions. In addition, we may also anticipate and monitor for clients’ complaints regarding service disruption.

**No unique identifier**

It is evident from both case studies that there is not a unique anomaly identifier for every attack step. We expect, however, that when we will enrich the attributes of the features of the detection system, most of the attack steps would be captured by different anomaly metrics. It should be noted that the anomaly metrics presented in this article are governed by the data sources that we currently work with. As further data sources become available, the extent of the anomaly metrics can be expanded. We would also expand the anomaly types related to files, to support the use of access, modification, creation and deletion. Physical building access can also be included based on logs that capture badge swipe activity for door entry – eg, as a ‘badge anomaly’.

Linking attack steps to anomaly metrics successfully provides the context for capturing behaviours of interest. Another dimension that can be extremely useful though, is the possibility of analysing the sequence of steps from the attack-pattern trees to determine new anomaly scores. As insiders obtain better knowledge of the detection systems in place and endeavour to mask their abnormal behaviours, it will be more difficult to compute effective anomaly scores. What may not flag as an anomaly when considering anomaly metrics individually, can be considered suspicious if a specific group of anomaly metrics are simultaneously high but not significantly enough to constitute an anomaly.

Consider the IP theft example and the attack-pattern tree presented in Figure 3. An attacker may choose to access sensitive files with their credentials, download them to a portable device and send a small portion of them via email to unauthorised parties. A sophisticated attack could be constructed in such a way that the size of the attachment of the email may not be significant enough to raise a flag in the email anomaly metric – the attacker may insert the portable device into a machine (the one that they usually connect to such devices) only once, and the downloaded files may be frequently browsed by them. If such an attack were to occur it would have been undetected by a system that considers anomaly metrics in isolation to each other. The fact, however, that an employee has scored high in three of the anomaly metrics (insert device, file download and email) and his actions are in such a sequence that form the identified path on the attack-pattern tree can be significant and constitute a specific type of anomalous behaviour.

In summary, we believe that attack-pattern trees comprise an effective framework that rationalises anomaly metrics but also provides further guidance for how combinations of metrics can be further related. Such a framework could be extremely useful in enhancing an analyst’s understanding, and additionally support the capabilities of detecting insider behaviour.

**Conclusion and future work**

Insiders who constitute a threat can have a significant impact on the systems, processes and data of an organisation and, ultimately, cause irreparable damage to its activities and reputation. As insiders obtain better knowledge of the detection
systems in place and mask their abnormal behaviours within their daily activities, it is increasingly difficult to design detection systems that will not rely only on computing scores for anomaly metrics in random, but will also identify potentially suspicious behaviours.

To tackle this problem we aimed to facilitate a better understanding of the threat at hand, through the presentation of a unifying framework to fully characterise insider attacks. In this article we expanded that framework and described a methodology leading to the identification of behaviours of interest. By adopting a grounded theory approach, we analysed and de-constructed 120 insider attack case studies to identify distinct activities that when combined form various types of insider threat. These activities, named attack steps, were used to reconstruct the case studies in order to design attack-pattern trees which highlight not only all the possible paths that an attacker can follow for a specific threat, but also denote the most prevalent of these paths.

Moreover, we provided guidance on how these attack steps can be linked to features and anomaly metrics identified in a detection system by applying the attack-pattern trees to two case studies, resulting in enriching the system’s effectiveness in highlighting interesting insider-threat behaviours.

It is straightforward to show that attack-trees and the anomaly metrics presented in this article cater for cases where only a single employee/actor is involved. We need to consider, though, how attack-pattern trees can provide insight to threats where several actors collude to accomplish an attack. Future work could focus on how attack-pattern trees, and specifically those that contain attack steps inferring the presence of other people, could provide guidance on combining different anomaly metrics to spot other people participating in the attack. We will explore the possibility of developing trees which show presence of more than one actor involved. Another avenue of future work could consider extending the attack-pattern trees by providing the motivational factors and the behavioural patterns that urge employees to become insider threats.

Acknowledgments
This research was conducted in the context of a collaborative project on Corporate Insider Threat Detection, sponsored by the UK National Cyber Security Programme in conjunction with the Centre for the Protection of National Infrastructure, whose support is gratefully acknowledged. The project brings together three departments of the University of Oxford, the University of Leicester and Cardiff University.

About the authors
Ioannis Agrafiotis is a post-doctoral researcher at the department of computer science at the University of Oxford and his research interests include human computer interaction, machine learning, and the use and development of formal methods. Prior to his post-doctoral experience, Agrafiotis completed his PhD at the University of Warwick, focusing on formal methods for information privacy. During his doctoral studies, he worked on the EnCoRe project through which he received an EPSRC studentship. He also holds an MSc in Analysis, Design and Management of Information Systems from the London School of Economics and Political Science and a BSc in Applied Informatics from the University of Macedonia, Greece.

Jason RC Nurse received his BSc in Computer Science and Accounting (UWI, Barbados, 2001), MSc in Internet Computing (Hull, UK, 2006) and PhD in Computer Science specialising in Web Services Security and e-Business (Warwick, UK, 2010). He has worked within industry and academia throughout his career. This has included various IT roles within industry, and academic posts such as research fellow at Warwick University, and more recently, cyber-security researcher at the University of Oxford. Nurse has published several articles at both journal and conference levels and also sits on the programme committee board of related venues. His research interests include insider threats, online security risks, information security and trust, human aspects of security, and services security.

Oliver Buckley received his BSc in Computer Science (University of Liverpool, 2004) and a PhD in Computer Science from Bangor University specialising in soft tissue deformation simulation using haptics and visualisation. He has experience within industry as a software engineer and also in academia. This has included working on the CITD project as a cyber-security researcher at the University of Oxford. He is currently employed as a lecturer at Cranfield University in the Defence Academy College of Management and Technology and is a member of the Cyber and Influence Research Group.

Philip A Legg is a post-doctoral research associate in the Cyber Security Centre at the University of Oxford. He works on the Corporate Insider Threat Detection project to develop novel techniques for the detection and prevention of insider threats. His interests span across several research areas, including machine learning, data visualisation, human-computer interaction and computer vision. Previously he worked at Swansea University exploring data visualisation for sports video analysis. Prior to this, he obtained both his BSc and his PhD in Computer Science from Cardiff University, where his research focused on multi-modal medical image registration.

Sadie Creese is professor of cyber-security in the Department of Computer Science at the University of Oxford. She is director of Oxford’s Cyber Security Centre, director of the Global Centre for Cyber Security Capacity Building at the Oxford Martin School, and a co-director of the Institute for the Future of Computing at the Oxford Martin School. Her research experience spans time in academia, industry and government. She is engaged in a broad portfolio of cyber-security research spanning situational awareness, visual analytics, risk propagation and communication, threat modelling and detection, network defence,
dependability and resilience, and formal analysis. She has numerous research collaborations with other disciplines and has been leading interdisciplinary research projects since 2003. Michael Goldsmith is a senior research fellow at the Department of Computer Science and Worcester College, Oxford. With a background in formal methods and concurrency theory, Goldsmith was one of the pioneers of automated crypto-protocol analysis. He has led research on a range of Technology Strategy Board and industrial or government-funded projects ranging from highly mathematical semantic models to multidisciplinary research at the social-technical interface. He is an associate director of the Cyber Security Centre, co-director of Oxford’s Centre for Doctoral Training in Cyber Security and Centre, co-director of Oxford’s Centre for Cyber Security Capacity-Building hosted at the Oxford Martin School, where he is an Oxford Martin Fellow.

References

5. Brdzicza, O; Liu, J; Price, B; Shen, J; Patil, A; Chow, R; Bart, E; Ducheneaut, N. ‘Proactive insider threat detection through graph learning and psychological context’. In IEEE Symposium on Security and Privacy Workshops (SPW), 2012.
7. Nurse, JRC; Buckley, O; Legg, PA; Goldsmith, M; Creeve, S; Wright, GR; Whitty, M. ‘Understanding insider threat: A framework for characterising attacks’. In Workshop on Research for Insider Threat (WRIT) held as part of the IEEE Computer Society Security and Privacy Workshops (SPW14), in conjunction with the IEEE Symposium on Security and Privacy (SP). IEEE, 2014.