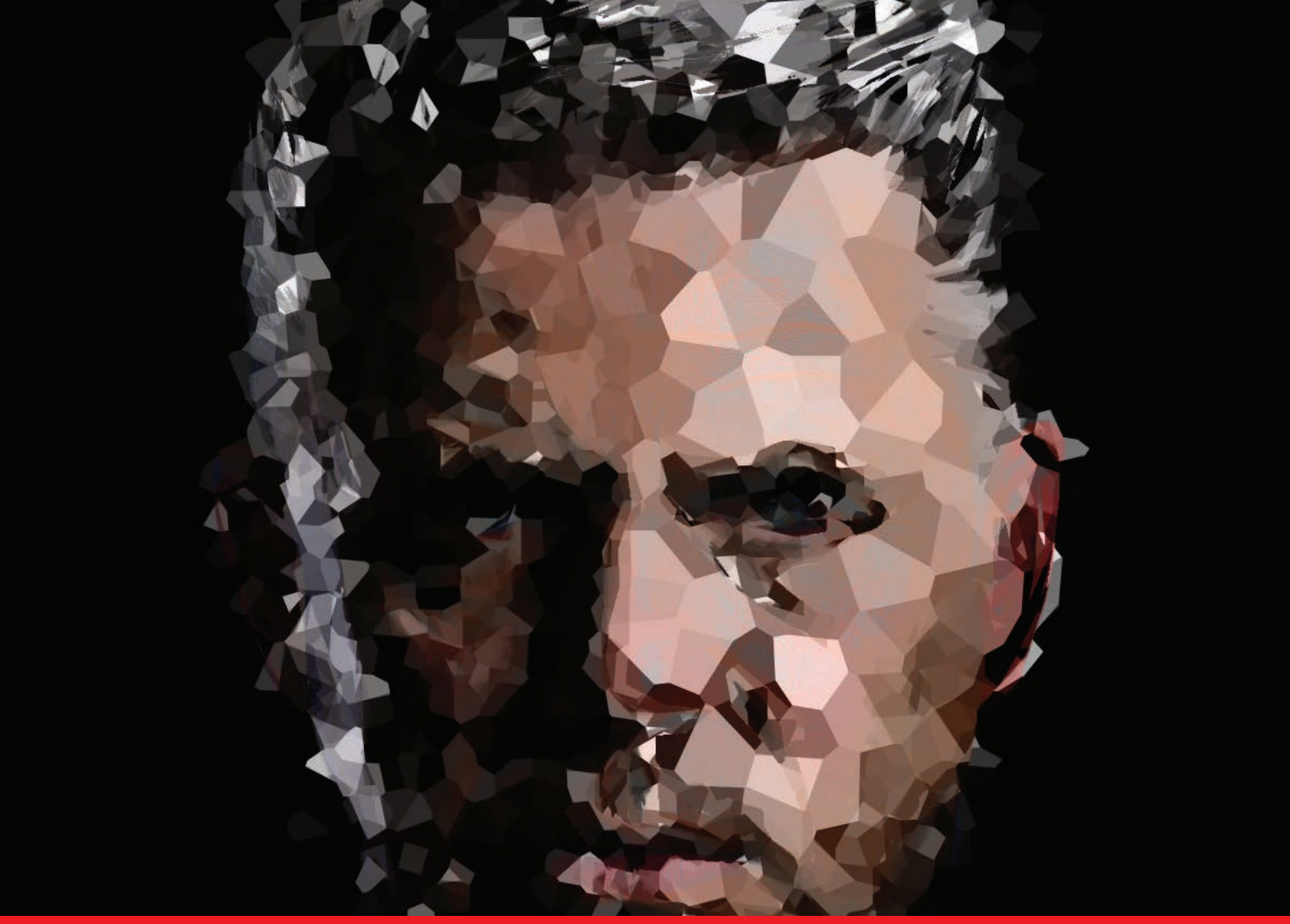


RED GOAT CYBER SECURITY
INSIDER THREAT REPORT 2019

RESEARCH RESULTS AND ANALYSIS

RED GOAT
CYBER SECURITY

Welcome

Welcome to the 2019 Red Goat Insider Threat Report.

Red Goat Cyber Security conducted this study into insider threat detection to discover what factors render people more or less liable to report suspicious activity. Through a sample of 1145 participants across a range of roles, countries and industries, we have gained a valuable insight into the barriers preventing reporting. The goal of this study is not just to provide you with evidence to drive change but also to put the severity and ubiquity of this problem into context.

We hope you find this report insightful, interesting and useful. We are very grateful to everyone who contributed and participated in this study - a great deal of insight was gained from your stories.

We also encourage you to get in touch with us if you have thoughts or questions about any of the findings identified in this research. Contact details can be found at the back of this report.

"This insider threat report provides a detailed insight and analysis of the issues plaguing insider threat programmes. It provides useful advice and guidance for improving your resilience against this growing threat."

Lisa Forte, Red Goat Cyber Security

Contents

Executive Summary

"Insider Threat" is an umbrella term used to describe someone who (knowingly or unknowingly) misuses legitimate access that results in or could result in damage to their employer. Insiders can act with or without actual intent to cause harm.

The risks posed by insiders are increasing as a result of our hyper-connected world. This steep rise in insider threat cases is caused by a number of factors:

- Improved access to organisational assets due to digitalisation of business;
- Expanding access to online marketplaces where data can be traded;
- Internet and social media providing people with access to individuals across the world; and
- Miniaturisation of storage devices and easier data duplication render exfiltration easier.

Insider threats are hugely complex to deal with and notoriously difficult to detect and stop. Colleagues are best placed to act as the company's eyes and ears by identifying and reporting suspicious activity. The issue is that we simply don't see this reporting happening until after the breach has occurred. By then it is too late.

Red Goat Cyber Security conducted this study into insider threat detection to discover what factors render people more or less liable to report suspicious activity. Through a sample of 1145 participants across a range of roles, countries and industries, we have gained a valuable insight into the barriers preventing reporting and the changes that need to be made to any organisation's insider threat programme. As leading experts in social engineering and insider threats, we seek to provide organisations with actionable data to drive their resilience programmes. The goal of this study is not just to provide you with evidence to drive change but also to put the severity and ubiquity of this problem into context.

The Results

- **There is a chronic under-reporting of suspicious behaviour for the majority of situations tested.**
- **Senior staff members are immune from being reported, irrespective of the severity of their actions.**
- **Contractors and new staff members are the most likely to be reported for suspicious behaviour.**
- **Participants favoured reporting to HR over Security teams and lack of training was found to be a major barrier to reporting. The qualitative data furnishes us with some colourful case studies to consider.**

The findings suggest some easy ways to improve your insider threat programme:

- Provide staff with adequate training on detection of concerning behaviours, why they are concerning and how to report;
- Ensure senior staff members sponsor the programme and encourage reporting of authority figures;
- Place HR front and centre as they were the favourite department to report to;
- Ensure that staff have confidence in the confidentiality of their report;
- Have clear guidance available of what needs to be reported so there is less ambiguity; and
- Start countering the narrative that, if you report someone, you will face reprisals

This research report will provide you with evidence, analysis and recommendations for developing your insider threat programme.

Introduction

Intentional Insider Threat (IIT)

This research is concerned with only one type of insider threat, the intentional insider. This covers all those insiders who act with intent against the company. Malice is one potential motivation to explain this intent but others - such as whistle-blowers, sabotage, espionage and simply a staff member leaving on their last day with a bag full of stolen reports that they worked on - are also observed. They all intend to cause harm, exfiltrate data or otherwise compromise the organisation.

Difficult to detect

The issue with intentional insider threats (IITs) is that they are notoriously difficult to detect and stop. Technical controls certainly have an important role to play but by themselves are insufficient. The best surveillance tool your company can deploy is your employees.

IITs will usually display ***"significant and sustained changes in their normal behaviour"***. With that said, the scientific community has not been able to find a single common profile or common set of behavioural indicators that would conclusively point to someone being an IIT. They have discovered that people with more narcissistic personalities may be more likely to become an IIT and that people with a higher level of intelligence are also more likely to become IITs.

The Problem: Reporting

The problem we decided to explore in our research was that, in all the cases involving intentional insider threats we examined, almost no reports of suspicious or abnormal behaviour were recorded about the insider threat actor in the weeks or months leading up to the breach. Yet, following the incident, there were large numbers of reports from colleagues describing concerning behaviour they had witnessed in the weeks and months leading up to the incident.

The level of internal reporting in companies and Governments around the world is poor. There are many explanations for this and, scientifically speaking, it follows the results of multiple studies into bystander apathy and intervention. Our research sought to discover what factors would render people more, or less, likely to report suspicious behaviour and clear wrong-doing.

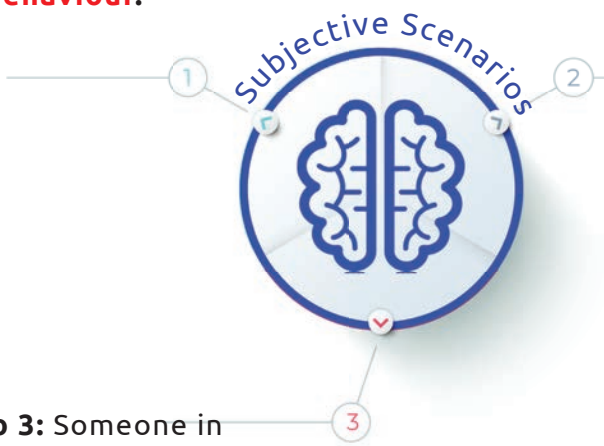
Methodology

Aim:
To examine when people will report other staff members and contractors and test what factors have the greatest impact on the likelihood of reporting resulting.

Methodology:
The sample size was **1145**. The sample represented a cross-section of industries and job roles. The study consisted of an online survey giving participants **five scenarios** to consider and a range of potential actions they could take. The five scenarios included three subjective and two objective scenarios. The subjective scenarios presented no hard evidence of wrongdoing and would be based on the opinion of the participants. The objective scenarios gave the participants more hard evidence of wrongdoing.

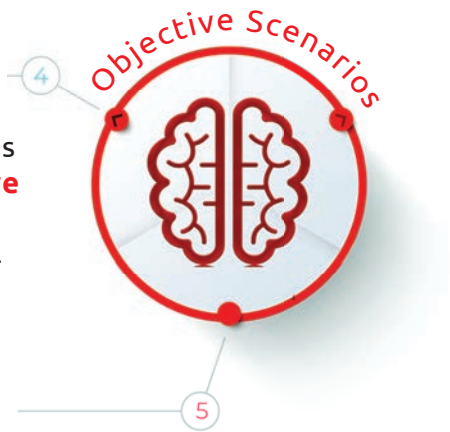
Scenario 1: Noticing that a staff member is, all of a sudden, displaying **withdrawn behaviour.**

Scenario 2: Noticing someone is displaying a **sudden and apparent increase in wealth and commitment** to their job.



Scenario 3: Someone in the organisation is being **vocally unhappy** about working there.

Scenario 4: Someone in the organisation has been **posting negative comments** about the organisation on social media



Scenario 5: Another member of staff has been **coming in late** once the rest of their team has gone home. They have also come in on Saturdays and last weekend they were **in the building with someone you didn't recognise.**

Methodology

Each scenario posed the following questions-

What would you do if the insider threat was:

- a **colleague**?
- a good **friend**?
- a **new member** of staff?
- a **senior member** of staff?
- a **contractor**?

In each scenario the participants had to decide which action to take. The actions fell into 3 categories:

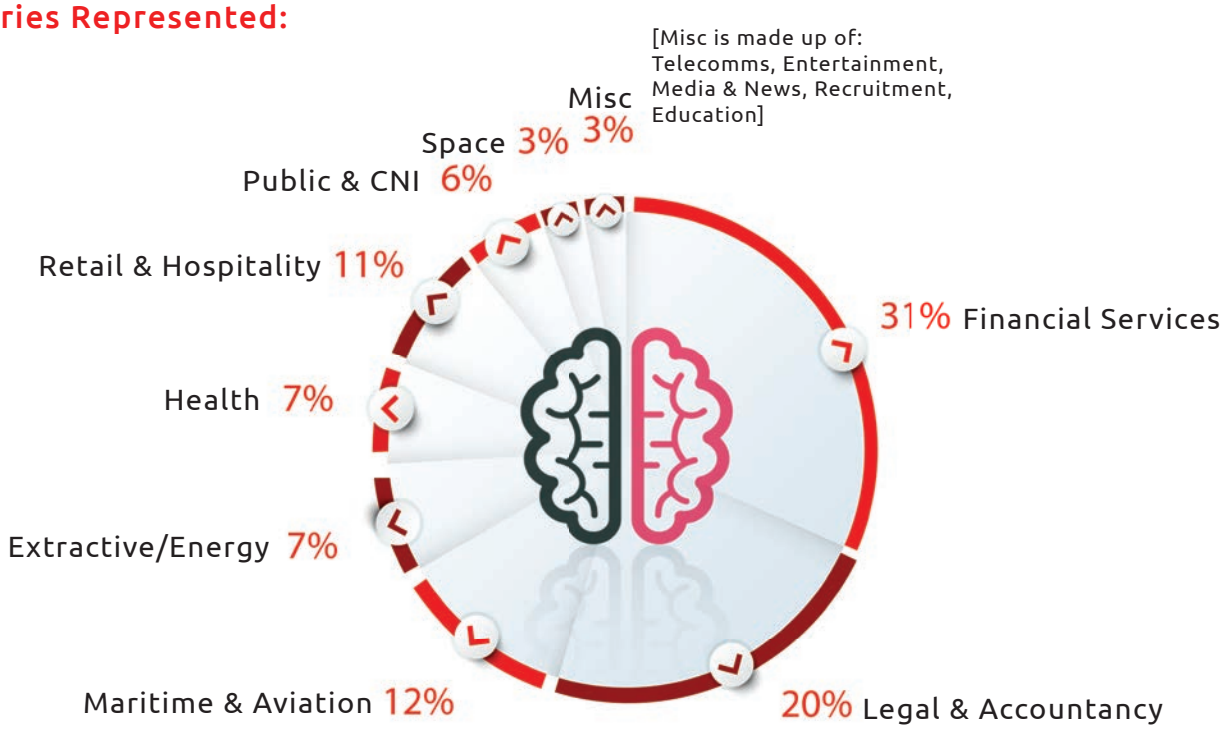
- **Take no action**
- **Report** it to **HR**
- **Report** it to your **Security team**

There was a free text box at the end for participants to expand on their answers or share experiences of incidents they had experienced.

Limitations:

As with all surveys, the results may be subject to social desirability bias. The low levels of overall reporting indicates that social desirability bias may not have had a strong influence on participants. The results, overall, were consistent with other research relating to elective acts by bystanders. The research also only examined the intentions of participants. Intention is a strong determinant of actual behaviour but other factors also play a role which were not tested.

Industries Represented:



Results Summary

THREAT ACTOR

1. Reporting was **less likely** across all five scenarios when the threat actor was a **colleague, friend or senior staff member**.

2. Participants were **more likely** to intervene when the potential threat actor was a **new member of staff or a contractor**. Indicating that employment status and length of employment play an important role in the decision to report.

3. Participants were **much less likely** to intervene when the threat actor held a **senior position** within the organisation.

4. Participants were **more likely to report their friends than they were other colleagues**. This indicates that people who are relatively unknown to the participants and people very well known to them would influence the likelihood of reporting in the same direction.

REPORTING PROCESS

5. When reporting was the selected action there was a clear preference to **report to HR** over the Security team.

6. Participants reported "**lack of knowledge and training**" as one of the largest barriers to reporting, indicating that belief that they lack the competence to identify concerning behaviours may stop intervention (obtained through qualitative data).

7. Participants reported an overall **lack of "confidence in confidentiality"** when it comes to reporting (qualitative data).

EVIDENTIAL LEVEL

8. Reporting was **more likely** in the scenarios where the **behavioural indicators were more obvious and objective** (scenarios four and five).

1. Reluctance to Report

Across all the scenarios there was clear and apparent under-reporting when the threat actor was a colleague, friend or senior staff member. Participants did decide to report their friends in the last scenario, however.

Figure 1: The percentage of respondents who would report each threat actor in the given scenarios.

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

What does this show?

There is a clear reluctance to report colleagues and senior staff members across all 5 scenarios. Even in scenario 5, which was the most objective and serious scenario, only 36% of participants would report a colleague and only 14% would report a senior staff member. There was a clear reluctance to report friends in scenarios 1-4. When it came to the more serious scenario 5, however, the reporting rate jumped from 19% to 71% of people who would report a friend.

What does this mean?

These results show a clear reluctance to report any suspicious activity, especially if the person in question is a colleague, friend or senior staff member. A substantial amount of scientific research has been conducted in this area. The chronic under-reporting found in our study can be explained by a consideration of the literature, case studies and qualitative data in this area that highlight the following barriers to reporting:

i) Benefits vs repercussions

Before the decision to intervene or report is made, individuals go through a cost/benefit analysis of the situation and the consequences for themselves. In society, there exists a cultural prohibition on reporting, a "code of civility" to which we all subscribe. This prevents people from reporting and represents a deterrent that has to be overcome for the reporter to feel that the act of reporting is worthwhile or safe.

Reporting is an elective act, hence a mere appeal to the broader issue of company security is unlikely to overcome this deep-rooted moral injunction against reporting others. Something far more powerful is required in order to overcome the deterrent. Jeffery Carney, a USA spy and double-agent, is quoted as saying:

> ***" If you want to do people with problems a favour…. and I'm speaking from experience – say something!"***

He goes on to claim that, if he himself had been reported, then he would have received help and wouldn't have become a double-agent.

1. Reluctance to Report

An examination of the qualitative data shows that an important consideration in the cost/ benefit analysis is whether someone's privacy and anonymity will be respected if they report.

Many comments suggest that there is a concern that they would be likely to face "reprisals" or perhaps even be "ostracised" from their teams for reporting. ***"I have ignored things that were obviously wrong in order to keep an easy life"***. Several commented that they would also fear being accused of discrimination if they reported a female colleague or a disabled colleague.

ii) Formation of an "anti-panic" mob

Research into the area of bystander-intervention has established that the number of "bystanders" to an incident is inversely proportional to the likelihood of one of them intervening. This has also been referred to as an "anti-panic mob". The majority of the participants in our study came from large and multinational organisations. These organisations often operate large, open-plan working environments, thereby creating a large number of bystanders or potential witnesses to the concerning behaviour being displayed by an individual. This may explain their willingness to take no action; after all, maybe another bystander will intervene instead.

iii) Every intervention follows the 5-stage model

Research by Latane and Darley proposes that for someone to intervene in any situation they proceed down a 5-stage model. Only when you reach the 5th and final stage do you actually report the issue.

Each of the 5 stages creates opportunities and barriers that could aid or impede reporting. For example, in a very busy office environment, it could be argued that the mere act of noticing strange behaviour might be unlikely to occur in the first place - in which case you may not even progress beyond stage 1.

Applying this framework to our qualitative data, it is apparent that the points at which the intervention appears aborted are stage 2 (participants relate not having the knowledge and training to identify what behaviours are concerning) and stage 4 (not knowing what they need to report and how to go about it).

From the qualitative data, it seems that the decision of whether to report is heavily influenced by self-interest and a level of self-preservation. People don't want to make their work life harder or be criticised for trying to do the right thing.

> ***" There is no benefit to me really, just huge negative consequences. It is a big personal risk..."***


“ I would rather come forward as a witness after the attack than risk my life and career being ruined by reporting it earlier.. ”

2. New Staff & Contractors

Participants were more likely to intervene when the potential threat actor was a new member of staff or a contractor.

Figure 2: Percentage of participants who would report new staff and contractors in the 5 scenarios compared to other actors.

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

What does this show?

Only a quarter of participants would report new staff in scenario 1 (the scenario that is most open to interpretation). After that we see a steady increase from 25% reporting in scenario 1 to 96% reporting in scenario 5.

The majority of participants chose to report contractors across all 5 scenarios; 67% of participants would report a contractor displaying withdrawn behaviour (scenario 1) and this then increases to 97% in scenario 5.

> ***" I feel like contractors and new staff could be anyone. It is more important for me to report them. "***

What does this mean?

New Staff

As a new starter in the organisation, it is likely that they are not yet viewed as part of the "tribe". As such the "code of civility" that prevents participants from reporting more long-standing colleagues is either weaker or does not apply to new starters. It may well be that the negative consequences associated with reporting are not as significant when the threat actor is a new staff member.

The qualitative data collected sheds further light on the result. Many participants explained their decision to report new members of staff by saying they "***were not vetted as long as other staff", "it wasn't clear who they are yet***" and "***you don't know if they are trustworthy until they have been here a long time***".

It is likely that, after a certain amount of time has lapsed, these new staff members would be treated like other colleagues or even friends and therefore be relatively immune from reporting.

2. New Staff & Contractors

What does this mean?

Contractors
Participants were especially eager to report contractors. Even in the first, most questionable scenario (withdrawn behaviour), 67% of participants would report a contractor.

Like new staff members, contractors are unlikely to be seen as part of the "tribe". This is evidenced by the fact that, in 3 of the 5 scenarios, over 90% of respondents said that they would report a contractor to either HR or Security.

The qualitative data paints a more detailed picture. "*I would report contractors without hesitation because they aren't part of your team. The consequences are limited". "Contractors have no loyalty to the company".*

> ***" I would be more likely to report contractors because I don't feel the consequences of it going wrong are as high as with colleagues. "***

Employment status and the length of employment seem to play an important role in the likelihood of reporting. It is likely that participants feel there are fewer negative consequences when the potential threat actor has not been at the organisation long or has a different employment status. However, Edward Snowden was a contractor. The colleagues that noticed a change in his behaviour refrained from reporting anything until after the NSA became aware of the breach.

3. Senior Staff are Untouchable

Participants were much less likely to intervene when the threat actor held a senior position within the organisation.

Figure 3: The percentage of participants who would report senior staff in the given scenarios compared to other actors.

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

What does this show?

The majority of participants refused to report senior members of staff. Even in the most serious and objective scenario (number 5), only 14% of participants would report a senior person.

What does this mean?

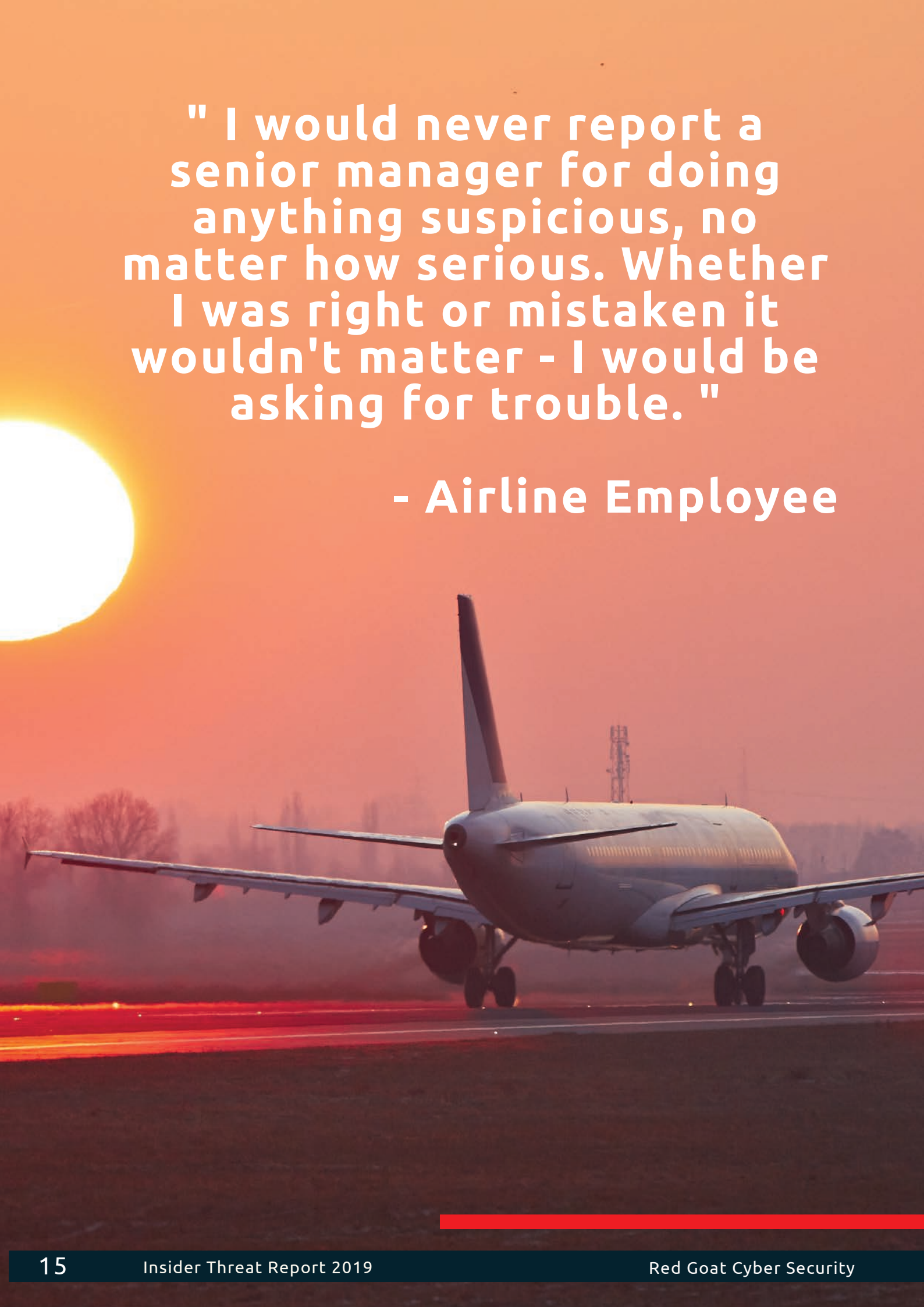
Senior staff members appear to be almost immune from being reported, even if their behaviour is obviously and objectively concerning. The hierarchical structure of most organisations creates a gap between the authority figures and the rest of the staff. The authority of senior staff is a remarkably persuasive force making staff feel unable to report them.

The qualitative data paints a darker picture of the problem. Participants reported: ***"It is an unspoken rule that, no matter what, you don't report a senior staff member"; "Rank means everyone above you is safe".***

Unlike the perceived consequences of reporting colleagues and friends, which seems to be centred around the creation of a difficult work environment, with senior staff things become more serious. The fear of reprisals now includes no promotion, decreased opportunities and ultimately being fired.

The troubling issue is that senior staff have more power, often better access and an increased scope for defining how they carry out their role. Yet one of the most effective tools for holding them accountable, other staff, is broken. Senior staff can do almost anything without fear of being reported.

> ***" Reporting a manager would end your career."***


" I would never report a senior manager for doing anything suspicious, no matter how serious. Whether I was right or mistaken it wouldn't matter - I would be asking for trouble. "
- Airline Employee

4. Reporting Friends

Participants were more likely to report their friends than they were other colleagues. The table shows the percentage of participants who would report their friends and other threat actors.

Figure 4: The percentage of participants who would report their friends in the given scenarios compared to other actors.

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

What does this show?

Participants are reluctant to report friends, colleagues and senior staff members in scenarios 1-3. However, in scenario 4, we saw- a higher rate of reporting friends (19%) than we did for senior staff (10%) and colleagues (13%). An even greater difference was shown in scenario 5 when 71% of participants said they would report their friend whereas only 36% would report colleagues and only 14% would report senior staff.

What does this mean?

Interestingly, this means that people unknown to the participants (new staff and contractors) and people very well-known indeed (friends) influence the likelihood of reporting in the same direction in the later, more objective scenarios.

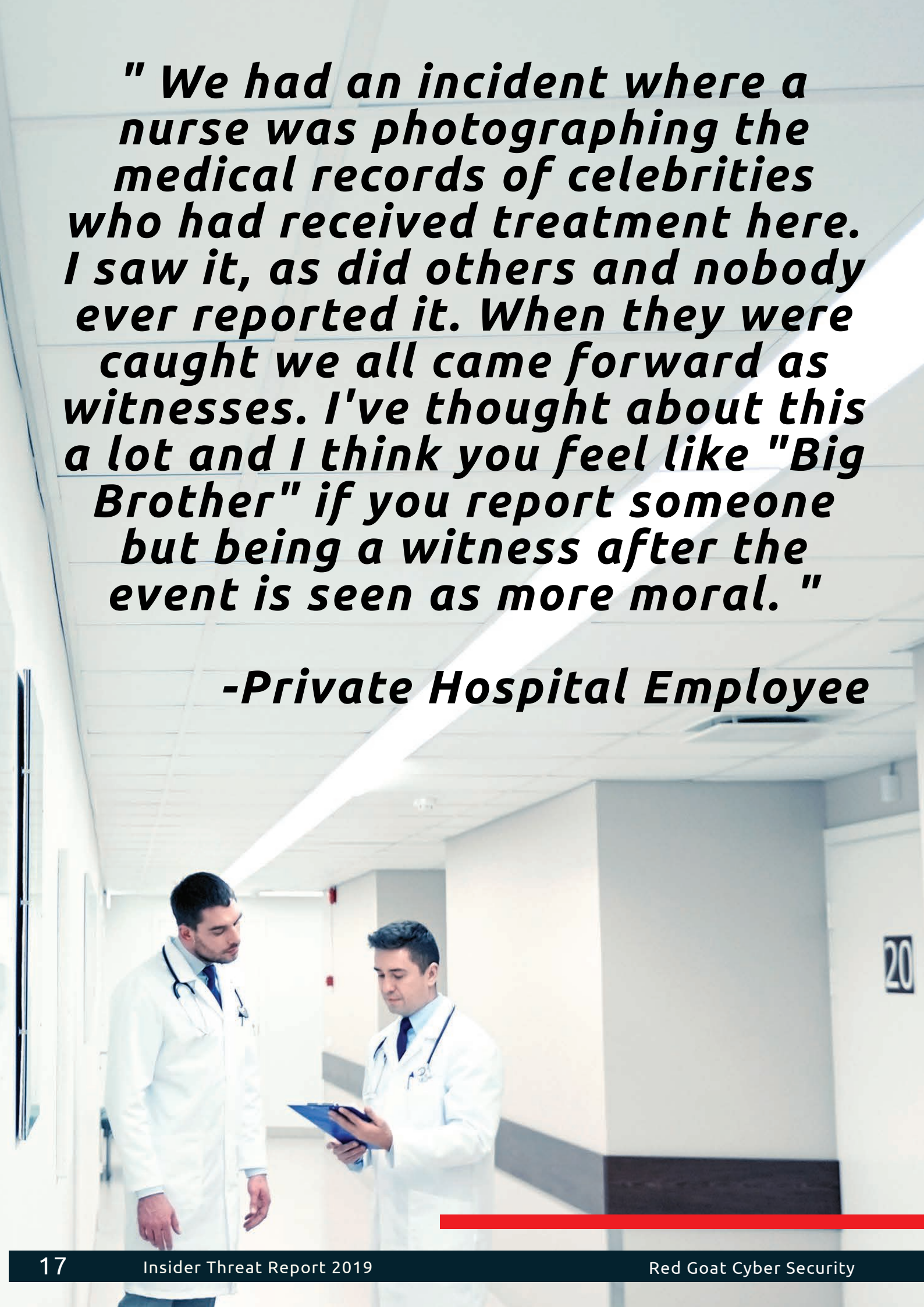
So why report your friends when you wouldn't report other colleagues? Participants reported ***"this could be a cry for help from my friend***"; and ***"Reporting my friend would likely help them in the long run"***. The qualitative data shows that participants may be justifying their action of reporting a friend as a helpful or caring act.

Although studies in other areas have found a similar result appearing this result came as a suprise to the research team and clearly requires further research.

> ***" I would make myself feel better about reporting my friend because it may be a cry for help. They are more likely to forgive me too."***

" We had an incident where a nurse was photographing the medical records of celebrities who had received treatment here. I saw it, as did others and nobody ever reported it. When they were caught we all came forward as witnesses. I've thought about this a lot and I think you feel like "Big Brother" if you report someone but being a witness after the event is seen as more moral. "

-Private Hospital Employee



5. HR Preferred for Reporting

Overall, with the exception of new staff and contractors, reporting was low. Of the participants that did decide to report people, we found that they preferred to report to HR.

Figure 5: Of the people who elected to report, the percentage who would report to HR or security.

Threat actor type	Scenario 1: Withdrawn behaviour observed		Scenario 2: increased wealth and commitment observed		Scenario 3: vocally unhappy staff member observed		Scenario 4: Staff member criticising company on social media		Scenario 5: unusual hours /bringing in unauthorised people	
	HR	SEC	HR	SEC	HR	SEC	HR	SEC	HR	SEC
Colleague	90%	10%	76%	24%	87%	13%	73%	27%	77%	23%
Friend	87%	13%	76%	24%	90%	10%	81%	19%	85%	15%
New Staff	97%	3%	96%	4%	96%	4%	85%	15%	67%	33%
Senior Staff	85%	15%	72%	28%	85%	15%	66%	34%	48%	52%
Contractor	86%	14%	89%	11%	85%	15%	71%	29%	54%	46%

What does this show?

There was a strong preference to report to HR over security teams across all 5 scenarios and all threat actors. There were two results where there was an almost 50/50 split in reporting to HR or security (senior staff and contractors in scenario 5).

What does this mean?

Participants clearly felt that HR was a more appropriate department for flagging their concerns. According to participants, ***"I would rather tell HR than security – they are far more likely to keep my report in confidence and handle it holistically instead of with an iron fist"*** and ***"I feel HR know about employees, the law and how to handle issues sensitively".***

Companies who have reporting procedures that do not involve the HR department may, therefore, be seeing a lower level of reporting that those that place HR front and centre.

> ***" I would rather tell HR than security – they are far more likely to keep my report in confidence and handle it holistically instead of with an iron fist. "***

6. Lack of Training is a Barrier

Participants reported a lack of knowledge and training as one of the largest barriers to reporting. Over 72% of the written responses cited a lack of training, knowledge and confidence as a reason why they felt unable to report suspicious behaviour.

> ***" I don't think my company has ever given us training on these threats. I'd feel more confident reporting if I knew what to look for."***

What does this mean?

Staff need to be clear and confident in identifying concerning behaviours, understanding why they are concerning and why they then need to be reported. The introduction of doubt or a lack of confidence will significantly increase the chance that the individual will ignore what they have seen. This knowledge base can only be achieved through training and awareness programmes.

Training is identified as one of the pillars of a successful and compliant insider threat programme. The United States Government has created a wealth of guidance on insider threats, all of which stress the importance of training.

This training is essential for the entire workforce but "high risk" roles should be focused on it to a greater extent. Intentional insiders need to be able to gain legitimate access to the sensitive assets of the organisation. The entire workforce is unlikely to possess such privileged access so organisations should be able to identify these "high risk" jobs for additional training. This also assists in reminding the workforce that assets created during the course of employment belong to the company and not the author. These assets should not be removed by the author on termination of employment as they belong to the organisation alone.

> ***" Our company just says report anything suspicious- there is no guidance, no training, nothing. "***

> ***" It is a scary thing to do [reporting]. I need some form of training and process otherwise I just feel like I am playing God..."***

" The guy that sat next to me would always be speaking on his mobile phone. Once he left his desk and I saw that it was actually recording a video. He quit a few days later and people were saying he had stolen some data. I should have acted but I doubted my judgement too much. "

- Investment Bank Employee

7. Reporting in Confidence

Participants reported an overall lack of "confidence in confidentiality" when it came to reporting.

There were extensive comments regarding concerns about a lack of confidentiality in reporting and fear of reprisals for reporting. Of the participants included in the qualitative data, 52% said they feared that their employer would not treat their report in a confidential manner.

> ***" If I were to report, everyone in the company would know by lunchtime. "***

> ***" I may even get into trouble just for reporting something. I don't want to be labelled a troublemaker...."***

What does this mean?

Every time someone considers reporting another staff member, they carry out a cost-benefit analysis in their mind. In most organisations the "benefit" of reporting (company security) is received only by the organisation and the "cost" is borne by the reporting individual. The costs are the fear of being ostracised and receiving reprisals. A "no fault reporting" policy is also crucial to encouraging this behaviour.

If staff believe that their report will be kept confidential, it is likely that the "costs" of reporting will decrease. As one participant noted, ***"we have a confidential helpline at work for mental health and counselling so why can't we have one for reporting these things?"*** Another participant observed ***"The bank I work at tells us the reporting is confidential, but it isn't really- it gets passed on to several different departments and they each ask questions so who knows how many people know by the end!"***

It is therefore important that staff have confidence that the organisation will keep their association with the report confidential and will not punish them for reporting. Confidential, no-fault reporting has to be an essential element for insider threat programmes.

> ***" People will know it was me. This means reporting isn't worth the risk. If I turn a blind eye and something bad happens, I will get another job or a pay-out. If I report, wrong or right, my life is ruined. "***

" I've seen Captains and others stealing, photographing documents and selling them. I have even seen people get paid to try and plug little boxes into ECDIS [Navigation system]. Thankfully nothing bad happened but I'm on a ship- if I report someone I am stuck with them for months! "

- Shipping Company Employee

8. Hard Evidence vs Opinion

Reporting was more likely in the scenarios where the behavioural indicators were more obvious and objective.

Scenarios 1-3 were designed to be more subjective and opinion-driven such as believing someone is displaying withdrawn behaviour. Scenarios 4-5 were designed to be more objective and evidence-based such as critical posts on social media or working late and letting unknown people into the office at odd hours.

Figure 6: Percentage of participants reporting each threat actor in the subjective scenarios (1-3) and objective scenarios (4 -5).

Threat actor type	Scenario 1: Withdrawn behaviour observed	Scenario 2: increased wealth and commitment observed	Scenario 3: vocally unhappy staff member observed	Scenario 4: Staff member criticising company on social media	Scenario 5: unusual hours / bringing in unauthorised people
Colleague	6%	7%	7%	13%	36%
Friend	5%	6%	7%	19%	71%
New Staff	25%	59%	81%	92%	96%
Senior Staff	7%	8%	8%	10%	14%
Contractor	67%	80%	91%	96%	97%

What does this show?

Across all threat actor types we saw an increase in reporting in the more objective, evidence-based scenarios. The greatest difference was observed when the threat actor was a friend: only 5% reported their friend in scenario 1 while 71% reported them in scenario 5.

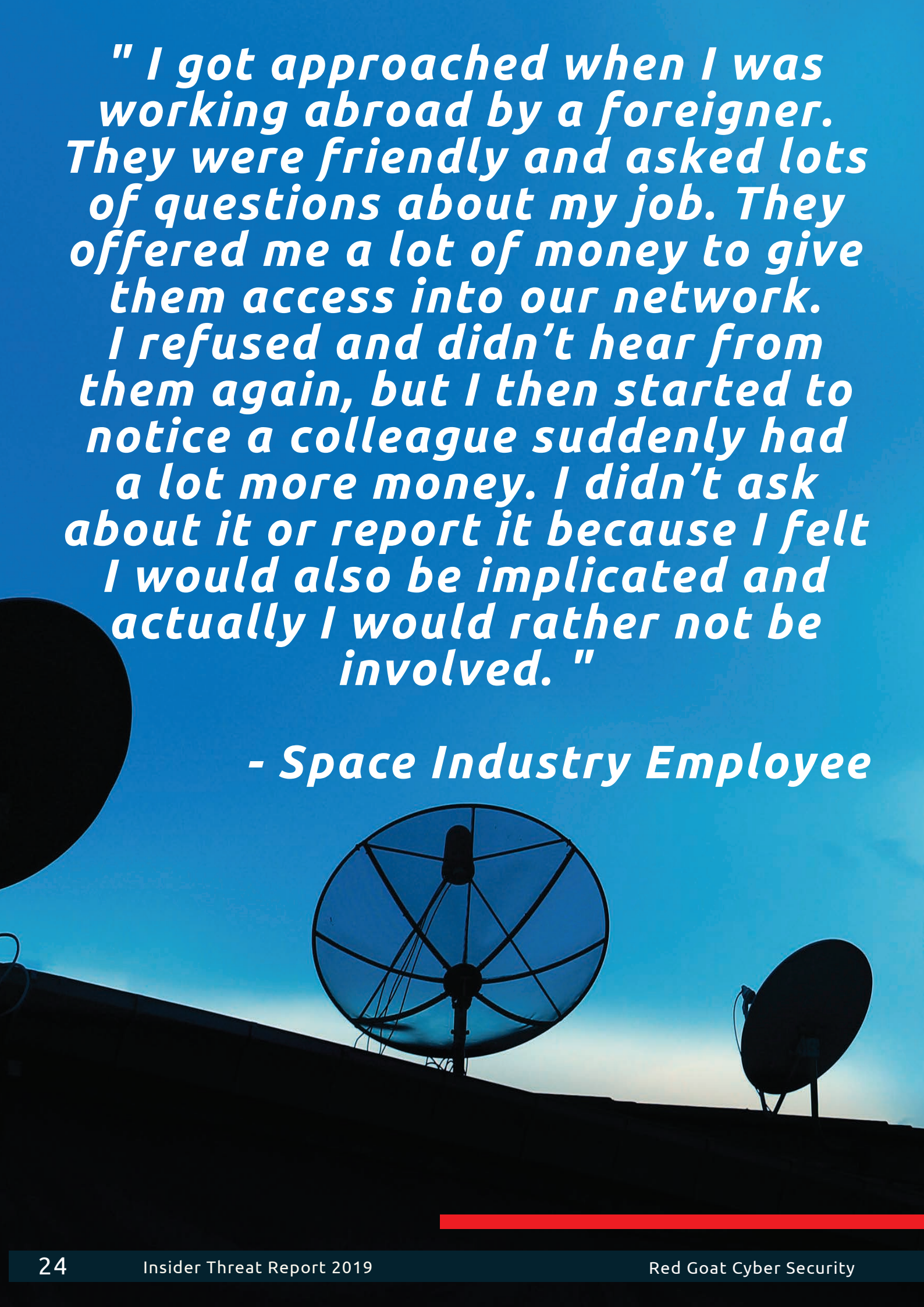
What does this mean?

This really supports finding number 6 (lack of knowledge hinders reporting rates). When you have objective evidence of wrongdoing in the form of screenshots of someone's social media posts, for instance, you do not feel there is as much scope for interpretation.

One thing this indicates is a need for training and company-wide guidance on the types of potentially concerning behaviours and why they need to be reported. The less ambiguous the company guidance on this, the more certain staff will feel in correctly identifying and reporting concerning actions. Our data shows that, when actions are less ambiguous and feel more objectively certain, people are more comfortable reporting.

It also points to a need for robust technical controls that could support staff reports with more objective evidence obtained from logs for instance. If they believe objective evidence could support their reports they may be more inclined to flag the concerning behaviour.

" I'd feel happier reporting if I had hard evidence, like a screenshot of their posts or something. Would I report someone just from my opinion of their behavior? Probably not."



" I got approached when I was working abroad by a foreigner. They were friendly and asked lots of questions about my job. They offered me a lot of money to give them access into our network. I refused and didn't hear from them again, but I then started to notice a colleague suddenly had a lot more money. I didn't ask about it or report it because I felt I would also be implicated and actually I would rather not be involved. "

- Space Industry Employee

Conclusion

Insider threats are becoming a growing concern worldwide. Increased connectivity has, inadvertently, made it easier for the intentional insider to pass on stolen data and be in contact with anyone from any corner of the world. The miniaturisation of storage and the digitalisation of records have also made it easier for people to copy and exfiltrate data.

Our findings paint a concerning picture when it comes to detecting intentional insider threats. The issue around reporting needs to be acknowledged by organisations and steps need to be taken to address it.

Chronic under-reporting

This study has demonstrated that organisations of all sizes and from a broad cross-section of industries suffer from chronic under-reporting of insider threat indicators. Even the high-profile cases of Snowden and Manning had colleagues approaching security the day after the breaches and giving evidence of their "concerning" behaviours in the days and weeks leading up to the breach. These cases gave rise to the notorious statement "Intentional insider threats are often observed and rarely reported". Under-reporting can be addressed through effective face-to-face training, clear policy guidance and a guarantee of confidentiality. Technical defences such as encryption and DLP are crucial in preventing attacks especially as under-reporting is so prolific.

Senior staff are immune

The belief that repercussions would be swift and severe meant that senior staff were effectively immune from being reported. This issue needs to be dealt with through top-down messaging and promotion of your insider threat programme.

HR is the department of choice

Without HR front and centre of your insider threat programme you could be seeing an even lower level of reporting. A participant highlighted that HR should be trained on the security implications of this threat. Similarly, training your security teams in relevant HR areas could also help "soften" their image in the organisation. Close working is vital.

Insider Threat Programme

Having an insider-threat programme is vital as a defence against intentional insiders. That programme needs to cover a number of important areas, including:

1. Training

Training is especially vital for people involved in the programme's creation including the security teams and HR. These people will be managing and leading the insider threat programme so investing in high quality face-to-face training is crucial.

Staff also need to be trained on what the concerning behaviours are, why they are concerning and how to report suspicious activity. The message that "security is everyone's business" should also be reinforced frequently.

2. Reporting Process

Reporting needs to be straight-forward and needs to ensure that staff have confidence in their confidentiality. Having set forms for reporting will also help ensure that staff furnish you with the information needed to progress the enquiry. A clear "no fault" reporting policy will help encourage the reporting of any security issues.

3. Building strategic partnerships

When developing your insider-threat programme, everyone's expertise in the company needs to be engaged. Insider threats are hugely complex threats that require a shared responsibility and burden.

4. Technical prevention

Ensure you have employed robust technical controls to prevent data exfiltration by insiders such as encryption and DLP. Ensure you log asset access where appropriate.

The insider threat can be challenging to combat as humans are hugely complex, displaying a matrix of emotions and motivations behind their actions. That said, although human beings have many differences, we all operate on the same hardware. Our behaviour has been extensively researched and our reactions, especially in groups, are largely predictable. This is why, with an effective insider-threat programme, your organisation can easily increase your resilience to this growing threat.

Expert Opinion

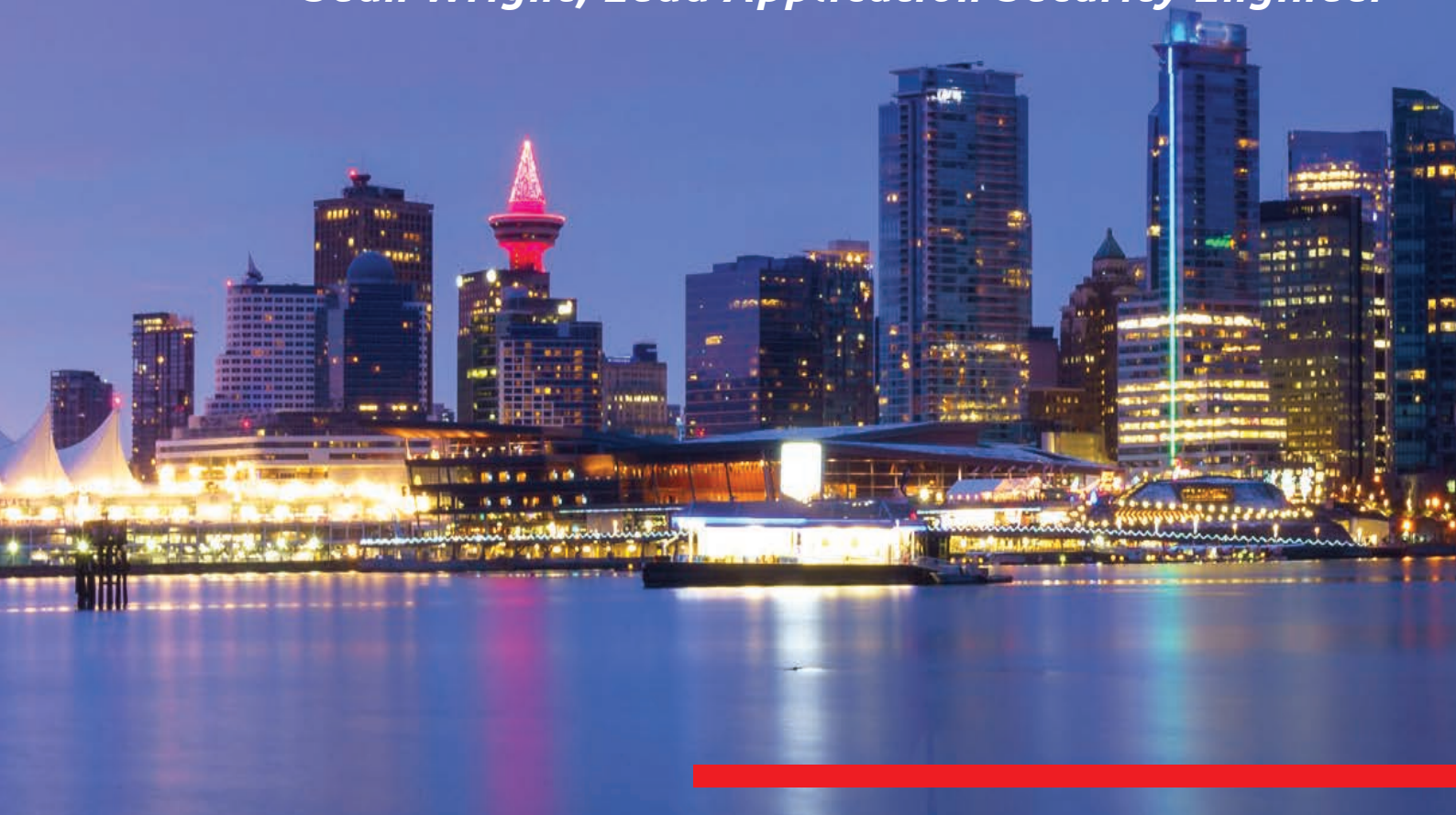
"Some insider threats can be very difficult to detect and even easy for employees to cover their actions. Some then go unnoticed for years. Mitigating such risk comes down to cleverly drawn up training programmes and a shift in culture which takes time."

- Jake Moore, Cyber Security Specialist, ESET

Expert Opinion

"An outsider is often looking for a way inside an organisation, and once inside, methods of escalating their privileges. Insiders already have access. Take a developer for example, they potentially have access to a wealth of resources and could bring enormous harm to an organisation."

- Sean Wright, Lead Application Security Engineer



References

Albrecht, Wernz, Williams Fraud: Bringing light to the dark side of business (1995).

Althebyan, Q., Panda, B.: A knowledge-base model for insider threat prediction. In: 2007 IEEE SMC Information Assurance and Security Workshop, pp. 239–246, June 2007 cited in Alhebaishi, Modeling and Mitigating the Insider Threat of Remote Administrators in Clouds, DBSec 2018: Data and Applications Security and Privacy XXXII pp 3-20,

Barron, J., Breaking the ring: the rise and fall of the walker family spy network. Avon Books; Reprint edition (July 1, 1988) (1987)

Bowes-Sperry, O'Leary-Kelly, To act or not to act: the dilemma faced by sexual harassment observers. Academy of Management Review, 30. (2005)

Buck, Rose, Crime Self-Reporting Study: Phase 1. 67. (2004).

Centre for the Protection of National Infrastructure, United Kingdom, https://www.cpni.gov.uk/insider-threat

Crawford,Bosshardt, Assessment of position factors that increase vulnerability to espionage. (https://apps.dtic.mil/dtic/tr/fulltext/u2/a293707.pdf) (1993)

Drucker, Beyond the revolution. The Atlantic. (www.theatlantic.com/magazine/archive/1999/10/beyond-the-information-revolution/304658/) (1999)

Giacalone,Discolsure of responsible behaviour: A review of proxy literature programs. [2001]

Ghumman, Ryan, Park, Religious harassment in the workplace: an examination of observer intervention. Journal of Organizational Behavior, 37. (2016)

Gueguen, Dupre, Georget, Senemeaud, Commitment, crime and the responsive bystander: effect of the commitment form and conformism. Psychology, Crime and Law, 21. (2015).

Keeney, Michelle & Kowalski, Eileen & Moore, Andrew & Shimeall, Timothy & Rogers, Stephanie. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. (2005).

Kowalski, Eileen & Conway, Tara & Keverline, Susan & Williams, Megan & Cappelli, Dawn & Willke, Bradford & Moore, Andrew. Insider threat study: Illicit cyber activity in the government sector. (2008)

Latane and Darley,The unresponsive bystander: why doesn't he help? New York, Appleton-Century Crofts, [1970]

Latane, Rodin A lady in distress: inhibiting effects of friends and strangers on bystander intervention. Journal of Experimental Social Psychology, 5. (1969).

NIST From Insider Threat To Insider Trust, https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/8.pdf

Randazzo, M.R., Keeney, Kowalski, Cappelli, Moore, Insider threat study: illicit cyber activity in the banking and finance sector. (2005)

Rogers, Bell, Pearce, The insider threat: behavioural indicators and factors influencing the likelihood of intervention. International Journal of Critical Infrastructure Protection, 24. [2018]. [Their research furnished us with the inspiration and template for this research]

Sackett,The structure of counterproductive workplace behaviours: dimensionality and relationships with facets of job performance. (2002).

Sarbin, Carney, Eoyang, Citizen espionage: studies in trust and betrayal. Praeger (30 April 1994) [1994].

Sarbin, Moral resistance to informing on co-workers (obtaining information from the workplace). [2001]

Sarkar, A., Khler, S., Riddle, S., Ludaescher, B., Bishop, M.: Insider attack identification and prevention using a declarative approach. In: 2014 IEEE Security and Privacy Workshops, pp. 265–276, May 2014, https://www.ieee-security.org/TC/SPW2014/papers/5103a265.PDF

Schwarz, Jennings, Petrillo, Kidd, Role of commitments in the decision to stop a theft. Journal of Social Psychology, 110. (1980).

Shaffer, Hendrick, Rogle, Intervention in the library: the effect of increased responsibility on a bystanders willingness to prevent a theft. Journal of Applied Social Psychology, 5. (1975).

Wood, Suzanne & C. Marshall-Mies, Joanne. Improving Supervisor and Coworker Reporting of Information of Security Concern. 80. (2003).

RED GOAT
CYBER SECURITY

Red Goat Cyber Security provides cyber security training, testing and crisis simulations to public and private clients across the world. As one of the leading experts in social engineering and insider threats, Red Goat provide world-class services to large and medium sized organisations spanning multiple industries. To learn more about the services Red Goat provide please visit our website or connect with us on Twitter or LinkedIn.

www.red-goat.com info@red-goat.com @RedGoatCyber (+44) 117 3259190