The insider threat has intensified as people have become increasingly mobile and hyper-connected. Almost every worker has multiple devices that can compromise information instantly and at scale: impact is no longer limited by the amount of paper someone can carry. Simultaneously, social norms are shifting, eroding loyalty between employers and employees. A job for life is being replaced by a portfolio of careers.

“Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls. Employees and negligence are the leading causes of security incidents but remain the least reported issue.”

– Experian Data Breach Industry Forecast

These shifts create challenges for organisations. The majority (89%) consider themselves vulnerable to insider threats; most (53%) include insider threats in their top three security concerns.

While estimates vary, ISF research has found that up to 54% of incidents reported in 2014 were a direct result of insider behaviour.

Most security professionals (62%) saw a rise in insider attacks over the same period.

Leading organisations across all sectors are looking for ways to address the evolving insider threat. Leaders who ignore or encourage inappropriate insider behaviour can expect financial, reputational or legal impact.

How do organisations determine who is trustworthy enough to be let inside – then build and maintain loyalty with a transient workforce? How do organisations manage risk while minimising costs related to vetting, security checks, and identity and access management?

Most research on the insider threat focuses on malicious behaviour; however, the threat is considerably broader. Insider negligence and insider accidents comprise a greater and growing proportion of information security incidents. CISOs who limit their thinking to malicious insiders may be miscalculating the risk.

This briefing paper equips ISF Members to combat the insider threat by:

– broadening the discussion to three types of risky insider behaviour: malicious, negligent and accidental
– describing the importance of trust and the central role it plays extending technical and management controls
– suggesting actions for immediate results and additional actions to sustain those results.

Finally, the paper asserts that organisations must work to foster a culture that improves trustworthiness itself.
Three types of risky insider behaviour

An insider is anyone who has been granted access to information and other assets that outsiders don't have. Insiders include current and former employees, contractors, business partners and suppliers. Insiders exhibit various behaviours, defined by the ISF as “the way in which one acts or conducts oneself, especially towards others”.

Consider the following examples of an insider threat being realised:

**Person M** decides to leave the organisation and, before giving notice, starts copying sensitive information to a personal drive.

**Person N** must work remotely to meet an important deadline, so uploads sensitive information to a free cloud service that is later breached.

**Person A** is repeatedly interrupted, and in haste sends an email containing sensitive information to the wrong recipients.

In all three examples:
- The person had access to sensitive information because of the privileges granted by the organisation.
- Sensitive information was compromised when it left the organisation inappropriately.
- The organisation was exposed to risk.
- The organisation trusted the person to protect the information.
- The person did not protect the information, or in other words, did not uphold the trust placed in them by the organisation.

The difference is that Person M behaved maliciously, Person N was negligent, and Person A's actions were accidental. These behaviours are shown in Figure 2 and described in more detail below.

**MALICIOUS**

Malicious behaviours require a motive to harm plus a conscious decision to act inappropriately. Examples include copying files before taking a job with a competitor, leaking confidential information, sabotaging networks, or using work privileges for personal benefit.

**NEGLIGENT**

Negligent behaviours do not have a motive to harm, but do have a conscious decision to act inappropriately. The act is usually well-intentioned — such as using unauthorised services or devices to save time, increase productivity or enable mobile working — and the behaviour often comes with the knowledge that the action is bypassing a control or circumventing policy. Despite the lack of malicious intent, negligent insiders are knowingly accepting risk that is outside the organisation's risk appetite.

**ACCIDENTAL**

Accidental behaviours have no motive to harm, and no conscious decision to act inappropriately. Emailing information to the wrong people, opening malicious attachments and publishing private data on public servers can all happen accidentally.

The first time someone behaves in one of these ways, it could be considered accidental; however, repeated accidental behaviour may also be considered negligent.

“A mistake repeated more than once is a decision.”
— Paulo Coelho

---

INSIDERS CAN BE COMPLICIT

Insiders can unknowingly facilitate the actions of malicious outsiders. By responding to phishing emails, for example, insiders can enable external attacks to succeed where they might otherwise fail. One organisation tested their employees by sending 150,000 fake phishing emails; nearly 50% of recipients clicked on the link within an hour.

Insiders can also intentionally assist external attackers. There have been instances where “seasonal, temporary or part-time workers used their short-term access to company systems and processes to assist outside actors in perpetrating substantial frauds. Once safely on the outside, their inside knowledge helps them manipulate their former co-workers and their former employer’s fraud prevention measures.”

FROM INSIDER THREAT TO INSIDER RISK

With some notable exceptions, the impact from information being compromised is similar, regardless of whether the insiders act maliciously, negligently or accidentally. In contrast, the likelihood can vary considerably, and depends on the complexity of people, including their motives, loyalties, ideologies and relationships with organisations.

To understand the risk posed by insiders, organisations must understand both the impact and likelihood of insider threats being realised, in other words, the impact and likelihood of trust not being upheld.

Trust sits at the epicentre of insider risk

Workers need privileges to perform their roles responsibly. A payroll manager (role) has an obligation to ensure employees are paid the correct amount (responsibility), which requires access to sensitive salary information (privilege).

There are limitations to these controls, so privileges always come with some degree of trust. Organisations are trusting that a payroll manager will not divulge salary data maliciously, negligently store it in an unauthorised cloud, or accidentally email it to a list of inappropriate recipients.

Organisations recognise they need to trust insiders to behave appropriately. Workers undergo background checks before starting, and may earn greater trust as their service and seniority increases. Organisations also require professional certifications for certain roles and provide training courses to equip their people with knowledge and skills to fulfil expectations of trust.

Organisations’ reliance on trust as a control has increased dramatically with advances in information technology and changing work environments. More and more people are being given long-term access to organisations’ critical systems – while there are more short-term contractors and it is “now more normal for staff to move between organisations and regions on a regular basis.”

How many organisations truly understand the aggregate risk from the trust they put in their people, from system administrators to everyone who is given a laptop?

---

UNDERSTANDING INSIDER RISK

While the insider threat is topical, organisations need to understand the risk it poses. The ISF defines risk as a function of impact and likelihood:

\[
\text{Risk} = \text{Likelihood} \times \text{Impact}
\]

ISF Member organisations are adept at estimating impact, supported by tools including the Business Impact Assessment and Business Impact Reference Table from the ISF Information Risk Assessment Methodology 2 (IRAM2).

Likelihood is more difficult to determine. The likelihood of an insider threat being realised can be thought of as the likelihood that an insider will behave in a way that does not uphold the trust placed in them.

Numerous factors influence whether or not trust will be upheld. Previous ISF research on the insider threat described a useful model examining what happens when people have motive, opportunity and means. These ideas can be extended by considering how trust plays a role in each type of risky behaviour.

Malicious

For malicious incidents, the breach of trust is often clear, as it was when an employee kept sensitive proprietary information after termination and provided it to a competitor where he became a paid consultant.

Whistleblowing is related; however, the intent tends to be based on ideologies or morals. Edward Snowden, who gathered and leaked classified documents on government surveillance, asserts that he acted out of loyalty to defend the US constitution from illegal acts, not out of malice toward his organisation.

Negligent

Negligent behaviours often occur when people look for ways to work around policies they feel hinder their ability to carry out their responsibilities. Insiders are expected to follow policy, but may also receive contradictory instructions, such as the need to meet a deadline or financial target.

“The number one most significant risk to every organization is your well-intentioned, non-malicious insider who is trying to do the right thing for the organization.”

– Jay Leek, CISO, Blackstone Group

Most workers recognise the importance of compliance and have a general awareness of security risks; unfortunately, their workarounds can be less secure than they realise. One worker justified violating policy and using unencrypted USB drives because they are easier to obtain and use than encrypted ones. He mistakenly believed that security could be preserved by simply deleting files after use.

Lack of oversight can rise to the level of a negligent insider risk, such as when a scandal uncovers that board members had no knowledge of widespread illegal activities.

Accidental

A large majority of ISF Members interviewed for this paper said that accidents were more common and of greater concern than malicious acts. Accidents also form a significant portion of information security incidents included in Verizon’s 2015 Data Breaches Incident report.

- Over 100,000 incidents are grouped into nine basic patterns, the largest of which is miscellaneous errors at just under 30%.
- Three of the top four categories of miscellaneous errors are accidental behaviours, including misdelivery, publishing error and disposal error.

Accidents can have significant consequences; one organisation was fined £120,000 after 11 unencrypted emails containing sensitive childcare information were sent to the wrong address.

ISF analysis of Verizon’s data suggests that 8.9% of incidents are because people cannot be relied upon to check the recipients before sending emails.

“IT professionals are far more concerned about ignorant users than any other group. 42% told us they considered them to be the greatest security risk in their organisation, ahead of tech savvy users who may be attempting to get around internal security protocols, or external visitors such as clients, customers and suppliers.”

– IS Decisions

Recommendations for managing insider risk

Managing risk posed by the insider threat should extend across all three types of risky behaviour: malicious, negligent and accidental. The recommendations in this section apply to all three; however, specific controls may be more applicable to some behaviours than others. The recommendations can be applied in whichever order is most appropriate for a given organisation.

Once the risk is assessed (Recommendation 1), immediate results can come from applying technical and management controls, and from aligning roles, responsibilities and privileges throughout the employment life cycle (Recommendations 2 – 3).

But that alone is insufficient. Organisations must foster a culture of trust, one where the organisation can trust its insiders – and insiders can trust the organisation in return (Recommendation 4). Organisations with a high exposure to insider risk should expand their insider threat programme to include the themes discussed in this paper (Recommendation 5).

1 ASSESS INSIDER RISK

Organisations that have not already assessed their exposure to insider risk may want to start by reviewing previous risk assessments using the perspectives provided in this paper.

IRAM2 can be used to assess insider risk. Phase C, Threat Profiling, provides a common threat list that is used to produce a prioritised threat landscape. The information risk practitioner could indicate which threat events from the threat event catalogue could be initiated by an insider.

In addition, IRAM2’s Phase C uses a risk factor called likelihood of initiation which is aligned with the “likelihood that insiders will not uphold the trust placed in them” described on page 4 of this paper. Because people are complex, information risk practitioners are advised to consult more widely when assessing trustworthiness. Ask specialists such as human resources teams, psychologists and other social scientists what psychometric or other assessments can help determine how IRAM2’s threat attributes, reproduced in Figure 5 below, can help determine the likelihood than an insider will behave inappropriately.

2 APPLY TECHNICAL AND MANAGEMENT CONTROLS

Research for this briefing paper found that there is an abundance of guidance on effective technical controls, although not all organisations have implemented basic first steps that include:

- identity and access management solutions
- desktop solutions that enforce data classification, for example by encrypting confidential documents before emailing, or by preventing highly confidential documents to be emailed to external addresses
- data loss prevention (DLP)
- event logging and monitoring
- remote wiping of mobile devices.

Technical controls should be supplemented by management controls such as reconciliation, segregation of duties, reviews, audits and so on.

Behavioural analytics and monitoring tools can develop a baseline of normal behaviour so abnormal behaviour can be detected. However, only 20% of firms continuously monitor user behaviour and proactively identify threats. Legal considerations must be taken into account when monitoring workers; many jurisdictions put limits on how intrusive monitoring can be, especially if people are singled out for monitoring before being accused of wrongdoing.

---

Figure 5: IRAM2: Threat attributes

<table>
<thead>
<tr>
<th>Threat attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability</td>
<td>How proficient is the threat and how well resourced is it?</td>
</tr>
<tr>
<td>Commitment</td>
<td>How skilled is this threat in terms of the execution of their role and interactions with information systems relating to the environment?</td>
</tr>
<tr>
<td>Competence</td>
<td>What is the general behaviour of the threat, and the culture of the environment in which it works? For example, is the threat conscious of information risks? Does the threat generally follow policies and procedures?</td>
</tr>
<tr>
<td>Culture</td>
<td>Is there a history of this type of threat having initiated threat events?</td>
</tr>
<tr>
<td>History</td>
<td>What is the nature of the threat actions this threat would take (i.e. Adversarial, Accidental or Environmental)?</td>
</tr>
<tr>
<td>Intent</td>
<td>To what extent is the threat driven to act against the organisation and the environment being assessed? For example, strong brand/reputation, socio-political influence, as identified in Phase A: Scoping.</td>
</tr>
<tr>
<td>Motivation</td>
<td>Is the origin of the threat internal or external to the organisation?</td>
</tr>
<tr>
<td>Origin</td>
<td>To what extent is the threat driven to act against the organisation and the environment being assessed? For example, strong brand/reputation, socio-political influence, as identified in Phase A: Scoping.</td>
</tr>
<tr>
<td>Predisposition</td>
<td>What would be the potential damage if events initiated by this threat were successful?</td>
</tr>
<tr>
<td>Privilege</td>
<td>What level of authorised access (logical and physical) does the threat have to the environment being assessed?</td>
</tr>
<tr>
<td>Severity</td>
<td>How potentially damaging could events initiated by the threat be?</td>
</tr>
</tbody>
</table>

### 3 ALIGN ROLES, RESPONSIBILITIES AND PRIVILEGES

When insiders have access to information they do not need, there is a mismatch between roles, responsibilities and privileges. This creates opportunities for insiders to abuse their privileges and compromise information.

Insider privileges vary from basic email and network access to highly restricted access given to subject matter experts and system administrators. The greater the access, the greater the impact if trust is not upheld, so insiders with more privilege may require greater security.

Privileges should be reassessed and unnecessary privileges revoked when roles and responsibilities change, as shown in Stage D of the employment life cycle (a human resources model that describes the stages of employment). When an insider departs, the organisation should disable all access, including non-core systems such as clients' systems and social media. There are many examples of data being compromised by people who still had access after leaving their organisations.

On a related point, Carnegie Mellon University found that “70 percent of insiders who stole intellectual property from an employer did so within 60 days of their termination from an organisation”. Organisations may consider revoking or reducing access before people leave; however, they should consider whether doing so undermines the culture of trust described in Recommendation 4.

It is useful to consider, at each stage of the employment life cycle, what trust the organisation is placing in people, and what can be done to reduce risk and improve trustworthiness.

The following list contains some potential controls.

**A Attract and recruit**
- Conduct pre-employment screening, vetting and security clearances.
- Include relevant clauses in employment contracts.
- Perform integrity checking of suppliers, contractors and other parties.

**B Induct**
- Ensure new people are equipped with the knowledge and skills to behave as secure insiders.
- Link expected information security behaviour to the overall norms and values of the organisation.

**C Evaluate**
- Include security and trust in supervision, performance management and appraisals.
- Ensure disciplinary policies contain clear and fair consequences for malicious, negligent and accidental insider behaviour.

**D Develop and change**
- Develop an anonymous reporting capability that workers can use if they observe behaviours that concern them and technical controls they might miss.

**E Exit**
- Revoke all physical and digital access credentials.
- If the insider was highly privileged, consider what can be done to verify that information has not been compromised.

All these actions can be supported by awareness and training, as described in the ISF report *From Promoting Awareness to Embedding Behaviours: Secure by choice, not by chance*.

“The when dealing with people, let us remember that we are not dealing with creatures of logic. We are dealing with creatures of emotion.” — Dale Carnegie
4 FOSTER A CULTURE OF TRUST

Organisations are trusting insiders to keep information safe, yet research found that less than half of workers (42%) believe it is their responsibility to do so.20

Make trust explicit

Tell insiders that the organisation trusts them. Be clear, when people join the organisation and whenever their roles change, that the organisation expects them to protect the information and systems to which they have access. State that they have a personal responsibility to uphold that trust, and make trustworthiness concrete by describing acceptable and unacceptable behaviours.

State the consequences of non-compliance. The organisation must act consistently and fairly when a person’s action or inaction abuses trust. Organisations with mature safety cultures (such as aviation and manufacturing) refer to a “just culture” where health and safety incidents are taken very seriously, people are individually responsible, and consequences are clear – but equally, every instance is dealt with fairly, recognising the effect that the organisation’s culture, processes and systems have to play in the incident.

Recognise that trust works both ways

Insiders are more likely to uphold the trust placed in them by the organisation if they feel they can trust the organisation in return. In fact, they expect it: “35% of people expect their company’s security settings to protect them against any risk”.21

Ensure the organisation, through its culture, management systems and processes, equips workers to fulfil the expectations of trust. For example:

- make it easy for workers to get the job done
- allow workers to talk openly about workarounds they might use and why they use them
- highlight risks associated with workarounds
- learn what workers need so secure alternatives can be provided22
- avoid contradictory instructions.

A culture of trust requires strong values, ethical behaviours, and consistent leadership actions (sometimes described as “tone from the top”), supported by transparent communications and safe feedback mechanisms.

The desire to improve trustworthiness is not limited to information security. In a 2015 CEO survey, “more than half of all respondents cited lack of trust as a barrier to their future growth prospects – up from 37% over the last two years”.23 Organisations are interested in knowing whether customers and the public view them as trustworthy, how trust impacts their brand, and how it can be measured and improved. CISOs and risk managers addressing the insider threat should discuss trust with those in the organisation who are working to, and can benefit from, improved trustworthiness.

5 EXPAND YOURINSIDER
THREAT PROGRAMME

Research for this paper found a variety of suggestions for insider threat programmes. They ranged from relatively straightforward programmes with basic steps (such as prevent, detect, respond) to Carnegie Mellon University’s “pattern-based approach” with 13 components, based on research from over 700 insider threat cases.24 25

Organisations choosing, developing and running insider threat programmes should ensure that the themes in this paper are addressed. If they are not, the insider threat programme should be expanded to ensure that:

- all three risky insider behaviours (malicious, negligent and accidental) are addressed
- insider risk is managed at all stages of the employee life cycle
- the organisation knows when it places trust in its insiders and how it can improve trustworthiness.

---

21 Ibid.
This paper extends the insider threat discussion beyond malicious behaviour to include negligent and accidental behaviour. It turns the spotlight on trust and the central role it plays in safeguarding information.

The trust organisations are placing in insiders has grown with advances in information technology, increasing information risk and changing work environments. This trend will continue as the volume of information insiders can access, store and transmit continues to soar – and mobile working for multiple employers become the status quo.

Leading organisations can combat the insider threat by implementing the recommendations in this paper.

Start by assessing insider risk. For immediate results, implement technical and management controls, and align roles, responsibilities and privileges throughout the employment life cycle.

Recognise that technical and management controls have limitations. Organisations need to trust their insiders to protect the information they handle – and will always face some risk of that trust not being upheld.

Embrace a deeper understanding of trust. Organisations must understand where and how they are trusting their insiders – and must augment technical and management controls by helping people to become more worthy of the trust placed in them. Equally, organisations should foster a culture that makes the organisation worthy of trust in return.

ISF Members have access to the ISF Members only ISF Live community where they can share innovative approaches and technologies that are being developed to address insider risk, including:

- a discussion about the use of security analytics to monitor insider behaviour
- a framework that may help organisations understand individuals’ propensity to attack, take risks or make mistakes
- further ideas for using IRAM2 to assess insider risk
CONTACT
For further information contact:

Steve Durbin
Managing Director, ISF

Email: steve.durbin@securityforum.org
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Web: www.securityforum.org
Twitter: @securityforum
LinkedIn: linkedin.com/groups/760947

Managing the Insider Threat:
Improving trustworthiness

ABOUT THE ISF
Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

Consultancy Services from the ISF provide Members and non-Members with the opportunity to purchase short-term professional support activities to supplement the implementation of ISF products.

WARNING
This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION
Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.