National Protective Security Authority

Insider events

A communications guide to reduce their impact

Be Insider Risk ready

Who we are

National Protective Security Authority (NPSA) is the UK Government's National Technical Authority for physical and personnel protective security, working to make the UK less vulnerable and more resilient to national security threats.

Contents

Introduction

Foreword by Kate Hartley 5

What's at stake

Introduction by NPSA 6

What is an insider event? 7

Communications toolkit

About our guidance 9

Research 11

Insider events need a different approach to crisis communication 12

Making sure your crisis communication plans work for insider events 13

Before an insider event 14

During an insider event 18

After an insider event 22

Dealing with different types of event 27

Unauthorised disclosure 28

Process corruption 30

Facilitated third-party access 32

Sabotage 34

Violence 36

The stages of a crisis

Crisis communications: a checklist 39

What the future holds

From NPSA 40

Further reading

References 43

Annexes

Annex 1 – Crisis communications: a checklist 44

Annex 2 – 'It's OK to Say' 47

Annex 3 – Insider crisis simulations 49

Annex 4 – Research findings 51

Introduction

Foreword

A member of staff passes confidential information to a competitor or a state actor, either for financial reward or for ideological reasons. Another is so disgruntled at work – possibly for reasons beyond your control – that they deliberately sabotage a core system, rendering your organisation unable to operate.

Kate Hartley
Author of 'Communicate in a Crisis: Understand, Engage and Influence Consumer Behaviour to Maximise Brand Trust'

Perhaps someone unwittingly gives an unauthorised user access to your organisation's confidential documents or accidentally leaves an unprotected laptop on the train.

Or perhaps one of your team developed cutting-edge technology but they've moved to a competitor, and they believe they have the right to take 'their' invention with them.

Whatever the motivation, insider events are increasing. And they're a very real threat to organisations. An increase in living costs, decreasing trust in official institutions, and the rise of online organised crime (including from state actors) all contribute to this often unrecognised threat.

NPSA's own research shows that leadership teams are concerned that their greatest threat could come from within. Civil unrest, cost pressures, increased criminality. These are just some of the themes expressed by senior leaders when asked about the possibility of an insider's actions causing financial, reputational or operational damage within their organisation.

And yet 60% do not have a plan to deal with it. Those that do, focus on technological solutions over the human ones. We need both. Mitigating the risk of an insider event means breaking down organisational silos, working with cross-functional teams to create a safe and open culture, great leadership and regular communication.

It gets to the heart of how an organisation operates and manages its people. Insider events are distinct from other types of possible crisis. It can tear people apart, have a lasting impact on culture, and destroy trust from within the organisation. It is not enough to rely on generic crisis communications principles to deal with it.

This guidance from NPSA has never been more important. It helps organisations embed their response to insider events into their crisis communications plans, with actions to take before, during and after an event.

Every organisation will have a crisis plan. It's time that plan included ways to address the threat from within.

What's at stake

Introduction by NPSA

Insider events pose a real and immediate threat to UK business and government. Your critical assets and systems – people, process, information, technology and infrastructure – are the lifeblood of your organisation, and these are under attack as the rate of insider events rises.

In response to this need, National Protective Security Authority (NPSA) has designed this guidance, the first of its kind, to help organisations thwart the threat and be ready.

If there are people in your organisation, there is insider risk

Our research shows that there are several factors driving the increase in insider events. Societal changes such as the squeeze on livelihoods, global instability and declining levels of trust in authority may all contribute. Furthermore, rapid digital transformation, which has spurred the acceleration of remote working and cloud-based networking, has made detection of incidents that much more difficult.

CERT National Insider Threat Center Carnegie Mellon Software Engineering Institute summed this up:[1]

"The threat of attack from insiders is real and substantial and our research consistently reveals that insider threats are a growing problem."

Given this environment, it's not surprising that our customers told us they were concerned by and sought support on how to reduce the risk posed by insiders, whether the damage they cause is accidental, malicious or, in their minds, justified.

The role of NPSA

We are the UK Government's National Technical Authority for physical and personnel protective security. Our role is to protect UK national security. We do this by helping organisations of all sizes and from all sectors to assess and mitigate security risks to their organisation, their (physical and intellectual) assets and their people.

As experts in protective security, we provide evidence-based guidance and advice to enable organisations to both understand their security needs and create their own tailored security protocols and procedures to thwart potential threats.

Think an insider event won't happen in your organisation? Think again

5 facts

1. The number of insider events has increased by almost half in just 2 years[2].
2. 98% of organisations feel vulnerable to insider attacks[3].
3. Malicious or criminal insiders were behind 1 in 4 incidents[4].
4. In EMEA, 21% of malicious insiders were related to espionage[5].
5. Events are taking longer and are more costly to contain – 3 months is average. The average cost of containment was estimated at over $15m at the time of writing, an increase over previous years[6].

What is an insider event?

People may be an organisation's most important asset, but they can also pose its greatest risk. The most serious insider-related events could include, "espionage, sabotage, terrorism, embezzlement, extortion, bribery and corruption" as well as "copyright violations, negligent use of classified data, fraud, unauthorised access to sensitive information and illicit communication with unauthorised recipients".[7]

An insider event is distinct to whistleblowing, which is a legitimate means of raising a public interest concern and is protected by law. Organisations need a process in place to express concerns.

NPSA definitions

Previously

An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.

An **insider**

Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology and facilities.

creates **insider risk**

The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.

can become an **insider threat**

An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation.

and cause an **insider event**

The activity conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

There are 5 main types of insider event:

1. Unauthorised disclosure of sensitive information
2. Process corruption (most likely fraud)
3. Aiding third-party access to an organisation's assets
4. Sabotage (physical, electronic or IT sabotage)
5. Physical threat (violence)

Communications toolkit

About our guidance

As part of our protective national security role, NPSA provides organisations with guidance on how to assess and implement mitigations to identified security risks, including those posed by insiders. Good personnel security practices can reduce the risk; however, insider events are rising and a multi-disciplinary team (comprising security, communications, HR and legal) needs to be ready to handle them.

Effective communication goes so much further than managing reputational risk. It can make an organisation less vulnerable to attack in the first place and, should an event occur, enhances how well it recovers relational trust, inside and out. After all, prevention is always better than cure, and insider events have the potential to create long-term damage.

Security professionals understand the risk that insider events present, but communication is often underutilised to mobilise staff as a first line of vigilance and deterrence.

That's why we have partnered with senior communication advisors to help develop guidance that looks at how an organisation communicates before, during and after an insider event. It seeks to inspire change in 2 ways:

1. To build a stronger bridge between the topic understanding held by security professionals and the engagement skills commanded by communication professionals.
2. To scrutinise existing crisis communication plans to ensure you are ready for an insider event.

The source of crises can be as much internal as external. Generic crisis best practice pays little attention to questions such as:

- How should an organisation respond when your own people are highlighting a shortcoming in governance, culture or behaviour?
- How to create messages that move your workforce to the desired outcomes?
- What's the best way to address subjective or ideological-based disagreements when rational facts may be less effective?
- How reliable is internal crisis monitoring when co-workers may not be open with how they really feel towards a trusted teammate?
- In what ways can you harness your people to rebuild relational trust as you bridge from failure to future forward?

Just as there is no one type of insider act, there is no single way to manage an insider event. Communication may differ in each context, but what it holds in common is the belief that your people are your organisation's most valuable asset – in need of trust, protection and support.

This guide is aimed at those involved in crisis communications management when the crisis is generated by an organisation's own people.

It's time to get comfortable with the uncomfortable truth – nobody is exempt from the threat. **If you have people, you have insider risk**, but when experts pull together, you become stronger.

Research

Research to inform this guidance

This guidance has been informed by primary research that included input from academics and practitioners with frontline experience of insider events, and desk research into how global media has covered the topic over a nine-year period.

Key recommendations:

1. The role of communication is a key thread for those striving to develop successful insider risk mitigation programmes. Communication should be integrated as much in the preparation and recovery of an insider event as it currently is around its management.
2. Efforts to mitigate and manage insider events are greatly enhanced through effective communication. Engaging communication draws on insight to prioritise the right message, delivered in the right tone, through a compelling messenger and medium to ensure it's understood and elicits the desired behaviour.
3. There is an opportunity to move from top-down "push" communication around threat to an engagement campaigning approach where success is defined by how well the message is received versus how widely it's delivered.
4. Insider events must be embedded into existing crisis best practices in a way that manages issues of fault, subjectivity and truth. Regular practice simulations are vital for building specific muscle memory.

Stronger, together

Greater collaboration between security and communication professionals enables a future where:

- every member of staff sees (and values) the role that they each play in helping reduce the likelihood of an insider event occurring
- communication enables vigilance and promotes deterrence across the lifecycle of an insider event, so that risk is anticipated not in pockets but throughout the organisation
- a connected organisation is better placed to mitigate, manage and ultimately recover from an event should it occur - this includes shared knowledge and sustained integrated practice

We're optimistic and it is our intention that incorporating some if not all the suggestions, will leave organisations more resilient in the face of the threat from inside.

Insider events need a different approach to crisis communication

Be insider risk-ready, or insider risk-sorry

Insider events raise distinct challenges for crisis communicators.

- By its nature, an insider incident surfaces organisational failure, calling into question issues of competency, culture and trust that need to be addressed as part of the issue
- The subjectivity behind insider motivations and lack of surety can make rational rebuttals challenging
- The relational impact on those inside and outside your organisation can be widespread. Internal strains can lessen your ability to pull together to counter the issue and may need longer-term attention. Externally, it can weaken critical relationships required to maintain competitive advantage

This raises questions about how to deploy communications to successfully mitigate, manage and recover from an insider event. Insider risk programmes often overlook communication or limit it to a 'promote' function. If this applies to your organisation's programmes, you may be more at risk than you think.

A crisis communication plan should be a core component of any organisation's risk preparations. Annex 1 provides a checklist and guidance on what every crisis plan should cover regardless of cause. These include clearly defined authority, action plan, assets and protocols.[8]

Assessing vulnerability to insider threat: key questions

1. Do you assess the impact of insider events based only on 'hard' organisational costs and financial impact, or do you consider 'softer' cultural, reputational and relational opportunity costs?
2. In monitoring and preparing for potential insider events, do you consider potential early warning signs that may surface from colleagues' concerning behaviours and how you might identify the manifestation of concerning behaviours in the workplace?
3. Have you planned for scenarios that address insider events as part of your crisis communication plans?
4. Do you rely too much on the formal elements of security communication (for instance, vetting, policies and discipline) at the expense of softer factors (such as culture, role clarity and expected behaviours)?
5. Are you keeping an eye on the evolving nature of insider threats as they relate to your organisation?

Are you taking a human-centric, behavioural and cultural approach to insider threat management – with strategic communication at its core?

Depending on your answers, you could be more vulnerable than you thought.

Making sure your crisis communication plans work for insider events

Look to address these aspects in your crisis communication plan

Before an event

Mitigate

Engage your workforce around insider threat and sustain an open culture via:

- culture of psychological safety
- knowledge and action on the warning signs
- employee engagement

Prepare

Ready your organisation in the face of an identified event breaking, through:

- auditing and prioritising vulnerabilities
- reinforcing organisational purpose and values
- stress-testing real scenarios

During an event

Manage

Systematically manage your plan including:

- sharing without impunity
- establishing strategic intent
- operationalising empathy
- engaging employees
- monitoring and relationship mapping
- uniting the impacted team

After an event

Recover

Have a structured learning review to re-establish trust and build resilience that:

- engages the team impacted
- encourages real openness
- declares the issue closed
- frames the issue, not the person
- doubles down on relational monitoring

The following pages expand on these points.

Before an insider event

Mitigate

NPSA's Insider Risk Management Framework (IRMF) helps you develop an insider threat programme to reduce that risk. Communication plays an important role in mobilising your workforce to detect and deter others, namely by:

- sustaining staff engagement as the frontline defence where they not only understand what an insider act is but actively see the role their behaviours play in prevention and are deterred from acting
- creating an environment where the workforce is aware of the concerning or unusual workplace behaviours which could lead to an insider event and feel able to speak out when something doesn't seem right
- enabling leadership at every level to model organisational values to reinforce the right behaviours and be consistent in how wrongdoing – whether malicious or accidental – is dealt with
- drawing on insightful use of language, channels and messengers to make communication impactful in inspiring behavioural change – the difference between receiving insider risk training and acting upon it

Culture of psychological safety

A strong security culture and a culture that feels psychologically safe – where staff feel engaged, included and comfortable to speak out – helps reduce the likelihood of an insider event occurring. A key characteristic of culture is good communication: how information is exchanged within an organisation, not just top-down but bottom-up and peer-to-peer. Communication is effective in role modelling. This includes not only celebrating best practice but acknowledging the truism 'you encourage what you tolerate', being firm on what is unacceptable.

Act on the signs

Insider events can take different forms, but they all have early warning signs among impacted teams. Develop a strategic communication plan to educate and train staff to recognise unusual or concerning workplace behaviour. The plan should educate your teams on HOW to report and connect with staff on an emotional level around WHY reporting is helping.

NPSA's 'It's OK to Say' programme helps organisations educate staff around how to identify and report unusual or concerning workplace behaviours, and in setting up mechanisms to promote the appropriate intervention. A comprehensive list of the things to watch out for is included in Annex 2, but these include:

- unusual or erratic behaviour
- staff disgruntlement
- a lack of intervention or lack of willingness to speak out by staff

Employee engagement

Engaged staff are more likely to say positive things about your organisation, remain committed to the team and put in additional time and effort when required.[9]

Higher engagement has been linked to increased profitability, productivity and innovation in the workplace, as well as low levels of staff turnover and absenteeism.[10] Communication disseminates information, but it also allows teams to extract the information they need, aids understanding, promotes community and generates debate.[11] Communicators should also pay attention to workforce satisfaction and engagement metrics as well as third-party reports. Listening to what critical audiences do (or don't) say about you can help identify your vulnerabilities.

Before an insider event

Prepare

We're looking specifically here at ways in which your communications team can build its resilience to manage an insider event should it occur. Looking specifically at insider events, crisis communication would:

- map and prioritise the insider risks that would most impact your organisation - radically listen for the materials that you would not want to be common knowledge inside or outside of the business, and rank them in terms of impact and likelihood, and develop specific communication plans for each
- apply your organisational purpose and values to your communication response, which will determine the actions that your team takes during a crisis and how you communicate
- stress-test your approach to specific scenarios by rehearsing responses to build organisational muscle memory

Audit and prioritise vulnerabilities

As a communicator, actively seek out the practices or materials that your organisation would not feel comfortable having shared widely inside or outside the organisation. Identify, prioritise and develop a communications plan for how you would respond if each of these were more widely released.

Continue this listening, without agenda outside your organisation and actively listen to what key audiences are (or are not) saying about your organisation to identify your vulnerabilities. Measures could include:

- regular threat monitoring using media, social media and staff listening tools
- staff satisfaction and engagement surveys to spot themes and early signs of discontent

Organisational purpose and values

Leading in ways that reflect your organisational purpose and values is desirable in all crises but is particularly important in insider-related ones, as trust in your competency, culture and relationships are challenged at the heart of the crisis.

Real-world scenarios, stress-tested

Having a crisis manual in place doesn't mean you're prepared for a crisis. Managing an insider event is no different. It's important to prepare teams with real-world scenario-based training to build human resilience.

Research suggests that 60% of organisations don't have an Insider Risk Management Plan in place and many are unsure how an insider event could impact them.

To help simulate a range of credible scenarios, NPSA has partnered with crisis communication experts to develop scenarios that can be customised to your organisation and the types of issues you may face.

The scenarios are customisable and include:

- unauthorised disclosure (activist and state actor-focused)
- sabotage
- violence

The materials can be used as the basis of flash card style discussion or as a live crisis simulation and learning review.

An overview of available materials is included in Annex 3.

Recap
How ready are you?

- Run regular insider risk training programmes involving all relevant functions of your organisation
- Make sure your crisis communication plans work for insider events by including insider threat in your crisis communication plan, which you should then review and update frequently, including the changing nature of potential threats
- Break down organisational silos for communication, and ensure communication is embedded in all organisational functions, pulling together leadership, HR, IT and other functions that could be impacted by an insider event – every role should have a deputy in case one or more of your core team is not available during the event
- Plan for different insider scenarios (see 'Dealing with different types of event', page 27), assess the likelihood of the risk and the impact, and consider what action you could take to avoid it altogether
- Run a live-fire insider crisis simulation, providing a high-pressure stress-test for your human preparedness and organisational resilience
- Use communications to reduce the risk of an insider event (that is, before the event, not just during) to include communications programmes to promote inclusion, culture, safety and risk awareness

Checklist

1. Communications team is integrated with operations within the business and has sight of key internal and external metrics. Deputies are appointed so the team is not reliant on one person.
2. An appropriate security culture has been built and is consistently reinforced.
3. Establish an insider risk programme that mobilises your workforce as your frontline in vigilance and deterrence.
4. Detailed plan is in place and the cross-functional team regularly tests it using relevant scenarios.
5. Your organisational purpose and values are socialised within the crisis team to drive all behaviours and accelerate decision-making across the organisation.

During an insider event

Communication during an insider event focuses on damage limitation. It should simply be the execution of the plans already developed in advance, but because an insider act is caused by one of your own, there is a greater need to:

- encourage sharing amongst workforce with impunity
- socialise your strategic intent
- think staff first
- operationalise empathy in everything that you do
- continue to listen through monitoring and relationship mapping
- unite the impacted team

Amnesty on sharing

Dependent on the incident and its severity, an investigation may be led by HR or by law enforcement. Where the police are involved, they will lead communication. Nothing you do should bias the outcome of that process.

Report the known facts and frame the issue not the individual. To encourage widespread fact gathering, you may consider an amnesty on information sharing with impunity. Teams should actively review all information shared, including reports that don't support the hypothesis being held, to establish a clearer understanding.

Strategic intent

Be clear on the desired end state for the crisis. Your strategic intent defines what great looks like and elevates your response beyond the short term, focusing instead on the actions that will deliver meaningful change. By their nature, they should have ambition framed within them.

After product sabotage that led to loss of life, a pharmaceutical brand defined its strategic intent as ensuring, 'nobody should ever die' from using its brand, which led to the tamper-resistant packaging breakthrough. Without this articulated intent, the actions taken might never have had the same scale of impact. Your values will inform your strategic intent. In the case of an insider event, action-inspiring examples could include, "I want everybody in our organisation to be safe" or "I want all of our people to have the quality of living they need, to bring their best selves to work."

Think staff first

An insider event will have a significant impact on your staff. Effective workforce communication is critical in building trust between your organisation and its workforce and in maintaining a culture of psychological safety.

Provide timely information – don't enable their information to come from outside sources. Remember, that what is said inside, should be considered an external communication.

Operationalise empathy

Demonstrably show that you care by matching expressed intent with quick actions that make a meaningful difference. Being physically and emotionally close to your audiences will help bridge the reputational and relational issues raised. For instance, if one of your values is 'we put our people first', it might translate into the behaviour,

> "That we are going to investigate rigorously and fairly and we will not pre-judge until more is known."

Relationship mapping

Put a system in place that enables you to categorise and prioritise critical audiences against the issues that matter to them. This helps you stay ahead of the curve by understanding their positions and likely actions. This is particularly valuable in an insider event where your staff may be asked to act in ways that conflict with the emotional relationships held with a potential insider.

Monitoring

Ongoing monitoring is critical in all crisis management phases, but during an insider event, it can be difficult to have an accurate read on internal sentiment. Being able to activate two-way, informal, peer-to-peer communication and trusted line management communication will help you identify messaging, approaches and behaviours that will help bring people with you. At this point, communication lines (peer-to-peer and trusted line management check-ins) become even more important in establishing what needs to be said and done to enable your desired outcome.

Unite the impacted team

The media often report what an act represents, more than what happened. A narrative-led approach can be effective in reframing the event in the context of the values important to the organisation. This helps root any ideological disagreement in the bigger issues. When countering an ideological-based justification for the action, communication that relies on rational facts and evidence is less effective. Moral foundations theory – the idea that people have enduring and intuitive morals that influence their worldview – would suggest you can build support by appealing to the unifying ideals that are shared by your organisation and workforce. You're not seeking to change the insider's view, but asking a series of open-ended questions as the basis for internal discussions may help build unity amongst those that previously sympathised with the perpetrator.

During an insider event

Recap
How ready are you?

- Assemble your crisis team, including deputies, and put the wheels in motion on your crisis plan
- Assess the severity of the event in terms of the impact now and potential impact in the future
- Set your intention for the event's outcome, in terms of what you want to happen as a result of the event, to inform your behaviour and thinking throughout the crisis
- Think staff first with your communications, as employee engagement is critical in uniting your team in line with your organisational goals
- In order to encourage staff to come forward with information or concerns, you'll need to be clear there will be no blame for mistakes made – consider anonymous information lines and support line management structures
- Prioritise your audiences and the appropriate channels to communicate with them – your first concern should be those most directly impacted by the crisis, but consider who else needs to be informed (for example regulators, insurers, investors, suppliers or the Information Commissioner's Office)?
- Set in place monitoring to keep on top of what people are saying about you during the crisis and to spot early signs of new threats, including in the media, on social media and through staff check-ins
- Communicate actions, not just intentions, so you make it clear what action you are taking to limit damage and to protect your organisation (and your workforce)

Checklist

1. You have a clear list of audience and stakeholders who could be impacted by the crisis and a plan to communicate with each.
2. Your statements and messages communicate action and are in line with your articulated strategic intent (and organisational purpose/values).
3. Staff trust the information that they receive from you and are open in coming forward with information and/or concerns. They understand what has happened and their role in limiting risk.
4. Monitoring systems are set up to help you identify reputational risks and sentiment.
5. Your crisis team is assembled, regrouping regularly with clearly identified roles.

After an insider event

The learning and recovery phase of any crisis is just as important in building ongoing resilience as any other. What's different about an insider-related incident is the far-reaching and often lasting relational impacts for co-workers, suppliers and partners in terms of lack of trust, confidence and self-belief. By surfacing your failure, they can also diminish the confidence of key external stakeholders.

As part of your structured learning review, the following additional measures help re-establish trust and increase your resilience for future incidents:

- undertake a learning review with the impacted teams
- active listening to surface the unspoken
- declare the issue closed
- frame the issue, not the person
- double down on relational monitoring
- focus on your recovery plan

Team-based learning review

Your teams' ability to understand how to move forward together after an insider event will not only deter and reduce the likelihood of repeat incidents occurring but it will be important in building trust and removing distrust. Undertake a learning review with the impacted teams to assess where systems might have enabled the situation to occur and deploy active listening to surface the unspoken.

Seek to understand, not be understood

When encouraging real openness, set aside proper time to engage with the teams impacted and consider doing this in a neutral space away from day-to-day distractions.

Consider sitting alongside each other rather than directly face to face. Be explicit about what you're seeking to achieve and how information gathered will be used when you're undertaking a learning review with the impacted team. Use open questions to encourage sharing and build mutual understanding. Examples might include:

- what is it like to experience this?
- how did you feel when...?
- how might we move on together?
- what would you like to see change/stay the same?

Use active listening techniques to show that you are listening to what is being said, and try to tease out what is not. Encourage verbal (mmm-hmmm, uh-huh, that's interesting, I understand) and non-verbal (nodding, smiling, eye contact) communication and don't be seen to offer judgement. Instead, reflect what you've heard (that sounds stressful, that must be hard, that must feel uncomfortable). Play back what you've heard to clarify understanding (so to me, that sounds like...). Ask multiple open follow-up questions. If you run out of allocated time, recap what you've heard and suggest a follow-up discussion to continue this conversation.

Declare the issue closed

Following your review, you may need to let teams know the process may take a while and that no news shared does not mean nothing is happening. When it's possible, declare the issue closed. Report what happened, the agreed next steps and make it clear that there is no further redress. Doing so brings the issue to an end and signals to individuals within your organisation who may have felt personally responsible or under scrutiny that they are a trusted part of the recovery.

Frame the issue, not the person

Throughout the process, be mindful of how language can alienate versus unite. Avoid implicit value judgements around guilt or causes. Be aware that even the term 'insider' itself is value laden. Consider 'alleged', 'accused', 'individual' as more neutral terms internally. Don't use jargon – speak in the team's own terms using plain English. Be mindful of the relational dynamic with the team left behind. Say only what you can see to be true. Consider using the internal copy check 'They were my friend' as your frame of reference. Does your communication pass this filter?

Double down on relationship mapping

As part of a systematic post-insider-event learning process, allocate responsibility for continuing your monitoring, listening and analytical activities to watch out for any 'aftershocks', which may require attention and action. Unlike other crises, the internal dynamic is so much more difficult to read through formal channels. Increase bottom-up and peer-to-peer communication to encourage open exchange.
Define who is responsible for regularly updating and reviewing your key organisational relationships grid for signs of stakeholder discontent.

Focus on your recovery plan

After the event is over, you will need to put in place a recovery plan to rebuild trust with your internal and external audiences. This is an opportunity to reinforce your values and behaviours and communicate the action you took to prevent the crisis happening again.[12]

After an insider event

Recap
How ready are you?

- Hold a team-based learning review in which you assess honestly what happened and how it happened, and what steps could be (or have already been) taken to avoid it happening again – this should involve your whole team, across organisational silos and encourage cross-functional thinking to suggest change
- Declaring the issue closed is an important part of moving forward and can help rebuild trust with partners, staff, customers and other stakeholders
- Focus on actions to avoid the threat in the future, and communicate what changes you have made to prevent a similar event happening again
- To focus on your recovery plan, consider ways to transfer trust into your organisation and hold yourself accountable to the commitments you made to change – remember, your communications may never go back to 'business as usual'
- Continue monitoring to pick up on any 'aftershocks' that result from the event

Checklist

1. The issue has been declared closed, so stakeholders know the threat has passed.
2. You have a defined process for conducting a structured post-insider-event debrief to identify the practical lessons learned.
3. Monitoring is in place to pick up aftershocks which may require attention and action.
4. You have a clearly defined programme for change and are communicating it to rebuild trust.


Fraud
2367.92
205.1
73.79
149.09
361.29
46.25
183.58
73.09
-14.89%
52.52%
35.12%
14.59%
18.49%
34.73%
-10.33%
24.29%
-11.00%
45.37%
11.54%
-18.09%
12.66%
9.35%

Dealing with different types of events

An inside look at insider events

Insider events take many forms, but they all have in common the fact that your own people are highlighting a failure of culture, operations or ethics.

The following pages, give consideration around how crisis communication would vary in each of the situations.

Guidance draws on detailed media analysis of insider events, academic learnings and the experiences of practitioners working on the front line of insider events.

Unauthorised disclosure

Unauthorised disclosure varies in form and severity – passing on sensitive information, leaking information externally (for example to a state actor or competitive organisation) and even accidental sharing, but at its root it is sharing privileged information without permission. It makes up almost half (47%) of all insider coverage reviewed over a nine-year period.[13]

Real-world examples

The phenomenon of 'leaking' information is culturally widespread and well understood. Made easier by newsrooms and social media, left unchecked in a team, it can create a more accepting leak culture, where the tolerance of selective leaks can embolden others to do the same.

However, unauthorised disclosure goes beyond revealing questionable information. A leading pharmaceutical company recently sued a departing member of staff for allegedly stealing 'scores' of confidential documents including those relating to its proprietary product technology. It was claimed that the individual uploaded more than 10,000 confidential documents without permission to personal devices. Analysis shows a steady rise in reporting of such permissive portability, particularly within technology and healthcare sectors, where individuals appear to treat corporate IP as if it were their own.

How unauthorised disclosure differs

- Possible delays in identifying the source of the crisis as an insider, this is particularly so where the media seek to protect their source
- The individual involved can often be incorrectly labelled as a whistleblower by the media, creating a more heroic (and sympathetic) narrative in support of their choices
- The information revealed can damage relationships with the very partners needed to help defend against the crisis
- Unstopped, information can form its own public discourse fuelling an outrage cycle where different groups publicly take opposing stands, which makes it much harder to establish your organisation as a single source of truth
- Containment can be less likely and, depending on the scale of perceived threat or controversy, can generate widespread and sustained third party commentary

Media learning

Where the individual was seen to be acting for their own personal gain, media coverage tends to view the organisation neutrally and the insider, more negatively.

However, in many cases media were found to misattribute the individual as a 'whistleblower'. In this case or where the organisation is deemed negligent in not stopping the questioned behaviour, it is more likely to be viewed negatively compared with other types of insider event.

How to manage communication

- Narratively, explain not what the disclosure was but what it represents (rigour, fairness and freedom)
- Monitor sentiment and its impacts on critical stakeholders – consider what additional reassurance is needed to restore the relational dynamic
- Take a human approach, communicating the impact on people ahead of profit or competitiveness, and demonstrate how the organisation is protecting those impacted by the disclosure, for example third-parties, staff or customers
- Demonstrate how systems and culture have been developed to prevent this from happening again

Process corruption

Process corruption (most notably, but not exclusively, fraud) is widely reported by the media and is one of the better understood types of insider event. Representing 36% of global data breach coverage,[13] the majority of media reports (68%) refer to financial gain. Aside from financial loss, impacts could harm staff morale and retention as well as cause reputational damage. While only one-fifth of fraud cases are believed to be reported,[14] it is estimated to cost the UK around £190 billion each year.[15]

Real-world examples

A former member of staff from a leading technology company was imprisoned for their part in an international bribery scheme which attempted to manipulate commerce through the platform. It was reported that the individual "used his inside knowledge" to hire staff to misuse their privileges and gain access to internal information, systems and tools. The illicit services undertaken included: stealing confidential business information relating to its IP, reinstating accounts and products that had been suspended, circumventing inventory fees, falsifying claims for lost inventory, and facilitating attacks on other vendors.

How process corruption differs

- It may be harder (and slower) to gather facts and deliver certainty of messaging from the outset – especially where the perpetrator knows the systems and is trusted
- The organisation decides whether to involve law enforcement agencies – those with fiduciary duties may need to report to regulators to protect shareholder interests and insurance companies may have a limited reporting window
- Where events bring national security risk, the National Crime Agency (NCA) or National Economic Crime Centre (NECC) may be involved – where there are criminal proceedings, communications will be led by law enforcement to ensure that internal proceedings do not prejudice the investigation
- The more trusted (more senior or expert) the suspected insider, the greater the questions raised about the organisational failings
- Containment may be less likely once external proceedings begin, but there will be lower levels of scrutiny as there is no immediate impact on public safety
- An organisation may choose not to acknowledge that an incident has occurred

Media learning

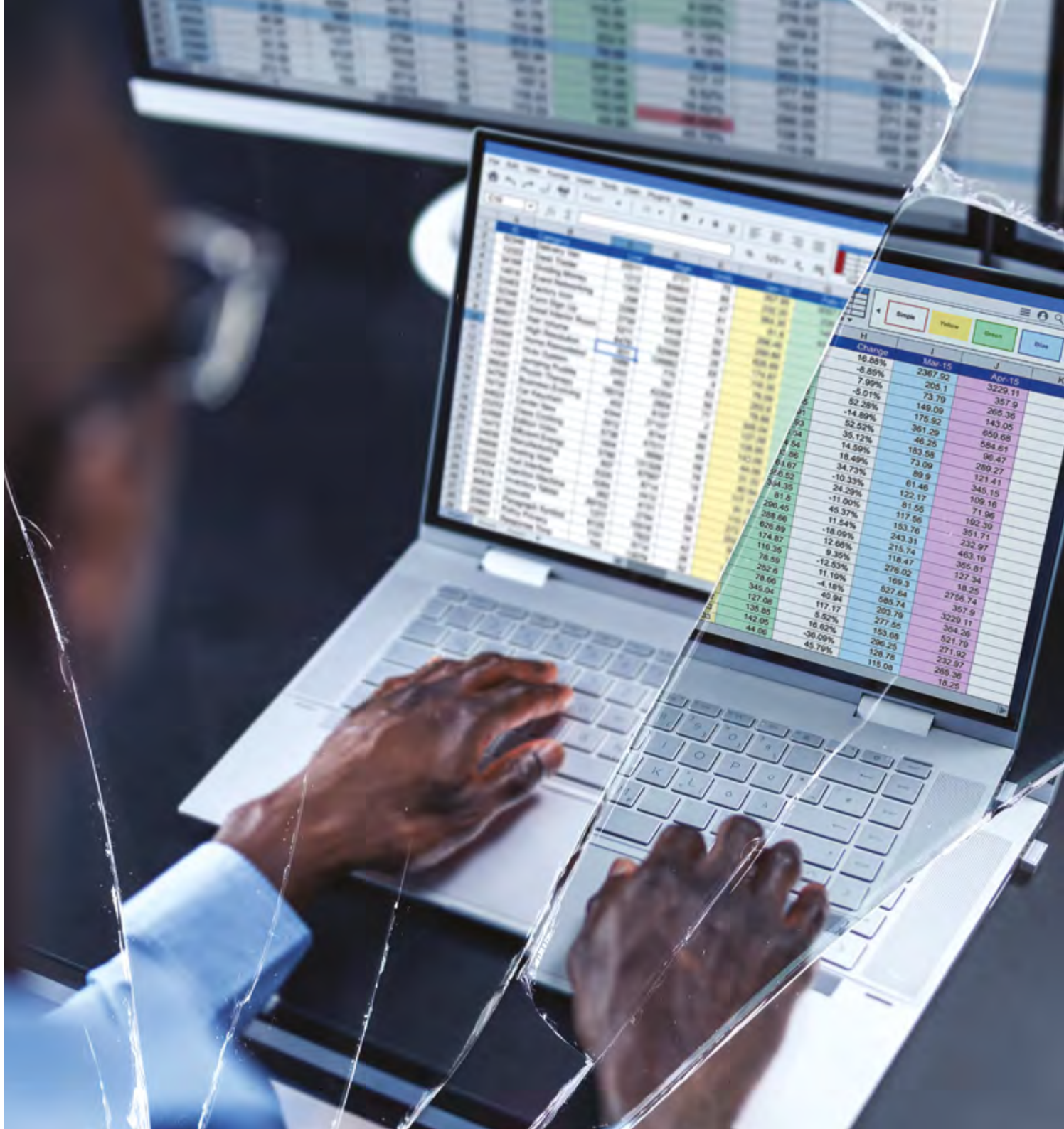
Motivations are complex and may not always be led by financial self-interest. Where the insider is perceived to be acting for personal gain, they are often portrayed by the media in a more negative light than the organisation itself. The exception is where the leadership is seen to be negligent (lacking strong financial controls or good governance) or acting in a manner where the insider's acts can be made to appear justified.

The organisation is likely to be viewed neutrally, but this can change if communication is poor or where a negative corporate culture was seen to cause the event. Leadership scrutiny can also be intensified at a time when its ability to speak freely is curtailed.

It can lessen confidence in the organisation's ability to protect other assets, making it important to reassure customers, stakeholders and suppliers of organisational competency.

How to manage communication

- Stick to the facts and prioritise the concerns that critical stakeholders might need addressing – avoid offering up opinions or speculations on motivation (this will come later)
- Demonstrate leadership values and competency through behaviour – communicate action rather than intention to show what you are doing to mitigate the risk of a future event
- Focus on staff communications first to limit the risk of a secondary event – encourage two-way engagement with staff to uncover further information
- Two-way communication helps reinforce a positive organisational culture – what you say will be taken as a measure of how you behave
- Establish the organisation as a single source of truth for staff and partners through regular two-way communication; consider a dedicated intranet page for the workforce, a help line for staff to call, and training to reassure on what worked well and how to embed new behaviours or processes – these will reassure stakeholders and curtail rumours
- Monitor sentiment among critical stakeholders to gauge what additional reassurance is needed to restore the relational dynamic
- Where others are impacted, clearly state when the event is 'closed' and service is resumed



Facilitated third-party access

Helping provide third-party access to an organisation's premises, information and people can hamper or, in the case of sabotage, halt your ability to operate and lead to losses of IP, revenue and even life as a direct or indirect consequence of the event. This creates both operational and reputational harm, throwing into question issues of organisational competency and trust.

Real-world examples

A Russian national pleaded guilty to conspiring to recruit a member of staff into a scheme to introduce malicious software into the company's computer network. According to court documents and admissions made in court, they conspired with others to recruit a member of staff to transmit malware provided by the conspirators into the company's computer network. Once the malware was installed, it was intended to exfiltrate data from the company's computer network and then extort the company by threatening to disclose the data. It is only the rapid response of the company in question which prevented a major exfiltration of its data.

How facilitated third-party access differs

- The organisation will need to fulfil its legal duties to report the event, and where there are criminal proceedings, communications will be led by law enforcement to ensure that internal proceedings do not prejudice the investigation
- The more trusted (more senior or expert) the suspected insider, the greater the questions raised about the organisational failings

Media learning

Media analysis of how insider events have been reported over a nine-year period, suggests that questions of organisational liability (and blame) have been increasing over that time period. We expect this to increase as media literacy of insider risk rises. Organisations should be prepared to defend the preventative measures put in place.

When insiders were malicious and the company was seen as a neutral party, sympathies tended to sit with the organisation. However, in cases of insider negligence, occasionally the organisation was seen to be at fault.

Our research also suggests that there's an enduring media interest in stories of trade secrets being lost, traded and stolen, particularly in top-tier international titles. This may be a result of staff actively trading access for espionage or personal gain and may suggest a lack of understanding about the risk associated with facilitating access freely.

How to manage communication

- Stick to the facts and prioritise the concerns that critical stakeholders might need addressing – avoid offering up opinions or speculations on motivation, but be clear to condemn the action of the insider
- Giving absolute clarity on what information has been exposed, with as much context as possible, will prevent the unnecessary panic or rumours that the access is worse than it is
- Communicate your fulfilment of legal responsibilities as part of the event
- Demonstrate leadership values and competency through clear action to limit current damage and limit the likelihood of future incidents
- Communicate the facts regularly to position yourself as a source of truth through the event
- Consider a dedicated intranet page for the workforce, a help line for impacted people to call and training on how to embed new behaviours or processes
- Correct misinformation and disinformation and beware of ‘follow-up’ events seeking to capitalise on the organisation’s perceived or real vulnerability
- Monitor sentiment and its impacts to gauge what additional reassurance is needed to restore the relational dynamic

Sabotage

Sabotage (physical or virtual) makes up one-fifth of identified insider event media coverage.[13] Sabotage has the potential to be both an organisational and a reputational crisis, creating long-term effects not just for your organisation but across its value chain. In some cases, this can go even further to impact the wider community in which it operates.

Real-world examples

A former member of staff from a global technology company pleaded guilty when charged with intentionally accessing its protected cloud infrastructure, without authorisation, to cause damage. Thousands of accounts were shut down for up to two weeks, resulting in millions of dollars incurred to restore the damage and refund affected customers. No customer data was compromised as a result of the defendant's conduct.

How sabotage differs

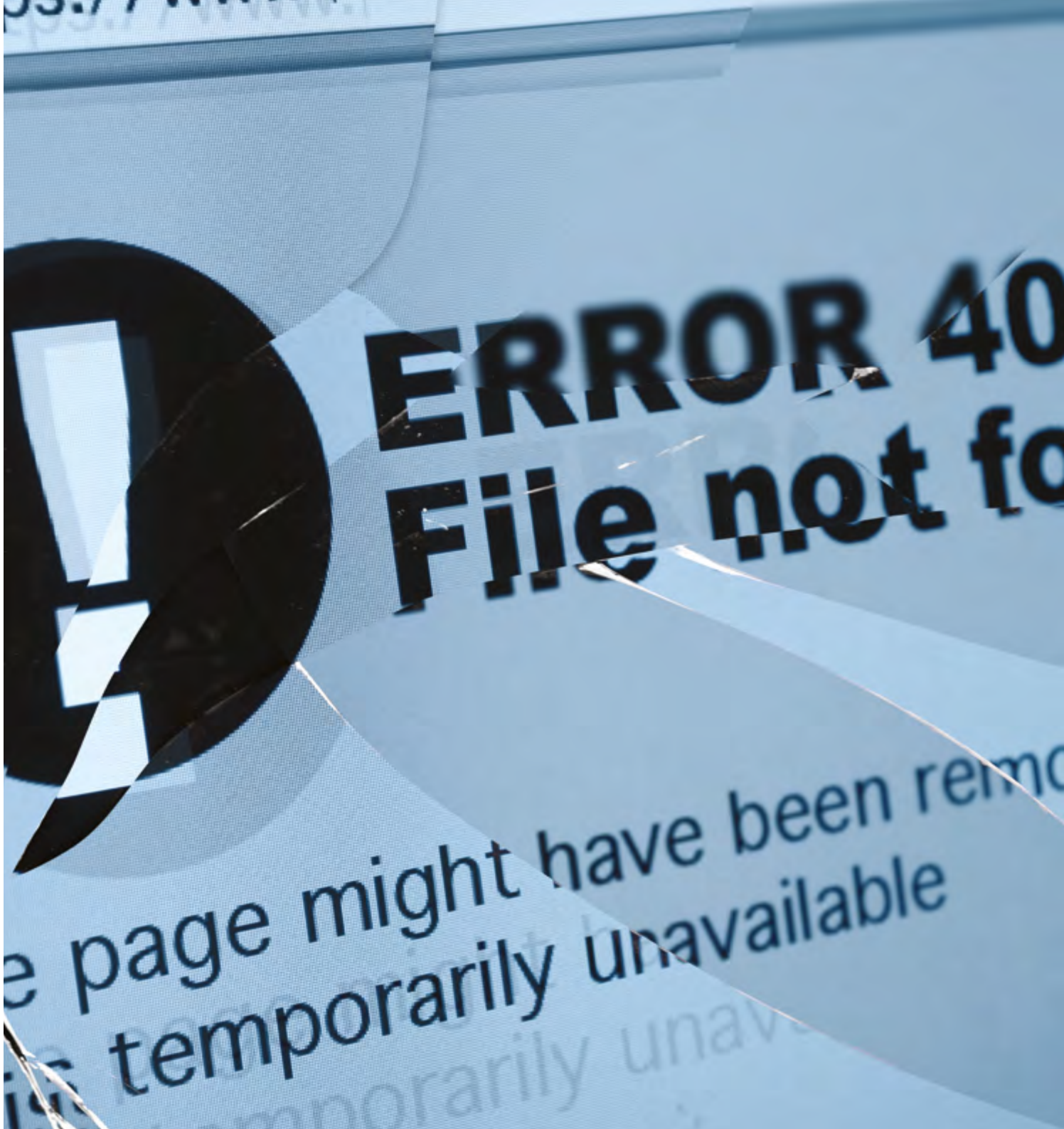
- Containment is less likely and, dependent on the scale of impact to third parties, can generate widespread and sustained third party commentary
- Where ideologically motivated or linked to staff member disgruntlement, your organisation may face scrutiny focusing on the circumstances that led to the attack
- It can quickly prevent an organisation from operating, bringing profound impacts across the value chain, placing burdens on customers, suppliers and consumers
- Where technology is sabotaged, it can compromise the very infrastructure required to respond to a crisis
- Sabotage is both a reputational and operational crisis – not only does it raise questions about reported ethical wrongdoing, it elevates concerns around your organisation's competency
- The visible impact on others and how it impacts your ability to operate as usual, brings higher levels of scrutiny, and where there is harm to human life, scrutiny is increased further

Media learning

Coverage reviewed frequently links sabotage with ideological-based conflict – a narrative that can make the insider appear heroic in their pursuit to thwart organisational policies deemed to be unethical, unpopular or undesirable.

How to manage communication

- Have back-up communication systems in place in case access is compromised
- Prioritise the harm that others may be experiencing and demonstrate empathy to their situation by sharing the recovery actions being put in place to return to normality
- Communicate swiftly with your workforce, and encourage open sharing of information that could lead to a greater understanding of the events leading to the sabotage (and uncover any further potential sabotage attempts)
- Delineate the insider event from a legitimate act, which might mean contextualising any grievance process followed and showing the mitigation support in place
- Communicate externally focusing on the facts of the event and its impact and what action is being taken to limit this impact – be clear that you condemn illegal action by the perpetrator and will act swiftly to prevent the event reoccurring
- Report only on what you see to be true, and avoid speculating on the individual or their suspected motivations
- Monitor media and social media sites for themes and sentiment and use this to frame future communication responses
- Clearly state when the event is ‘closed’ and systems are back up and running



Violence

Insider violence includes any action or threat of physical violence, harassment, sexual harassment, intimidation, bullying or other threatening behaviour by a co-worker in the workplace.

Reported incidences in the UK are rare, with data suggesting it affects 1.4% of men and women in England and Wales, representing 299,000 assaults and 389,000 threats in 2019/2020.[16] Incidents may be rare, but they are highly traumatic, visible and, in the majority of cases, there are warning signs in advance. A US report on pre-attack behaviours of active shooters suggested that nearly two-thirds (62%) were found to have a history of acting in a 'harassing, abusive or oppressive manner'.[17]

Violent insider events create an intimidating, hostile or abusive environment where individuals are not willing to speak openly for fear of reprisal. At their most extreme, they can result in loss of life.

Real-world examples

A former member of staff killed a number of people on site during a shooting incident that lasted less than four minutes. The building was equipped with metal detectors and security turnstiles at its entrance and employment badges were required to gain authorised access. The family of the victims raised a legal suit for wrongful death, claiming that the attack was 'preventable'. The perpetrator was known to law enforcement officials.

How violence differs

- It is very clear very quickly that a crisis is in place
- Scrutiny will be higher as it involves public safety
- A wider range of stakeholders may be involved (including emergency services, law enforcement, occupational health)
- Information is harder to get (and verify), and the police will take the lead
- Where there is human harm, media interest will be ramped up domestically (and even internationally), so speed of response is critical

Media learning

Violence will result in high levels of media interest. The insider is likely to be portrayed negatively within the media. High levels of public interest may dictate how journalists report the story. In the UK and Ireland, journalists are held by the NUJ code of conduct (2018) which states, that "a journalist obtains material by honest, straightforward means with the exception of investigations that are both overwhelmingly in the public interest..." and "does nothing to intrude into anybody's private life, grief or distress unless justified by overriding consideration of the public interest."

Their need to explain what may seem inexplicable may involve reducing complex (and often unknown) insider motivations into a simplified, singular explanation. In the absence of footage, they will seek third-party testimony to paint a portrait of the insider's experiences by means of explanation. The organisation is likely to be viewed sympathetically, but this can change if communication is poor or where the organisation is deemed to be culpable.

How to manage communication

- Prioritise providing help and reassurance to those impacted – the injured, co-workers and relatives
- Communication should avoid messages that create panic
- Work closely with law enforcement to avoid communicating anything that could impede a criminal investigation
- In keeping with NPSA's crisis communication guidance for a terrorist attack,[18] look after your communications team as they are likely to need back up drawn from elsewhere in the business; send some of your team home as soon as the incident hits, it will be hard for them, but you will need at least one experienced communications lead for every shift
- Think carefully about what staff may see when visiting the incident site – it may not be necessary to send a member of staff to the site; however, if a visit is necessary, it is often valuable to buddy up a communications team member with an operational member of staff or member of your security team
- The trauma will be felt equally by staff and members of the communications team – consider providing ongoing professional counselling support
- Clearly state when the event is 'closed', the investigation is complete and the facilities are open again

The stages of a crisis

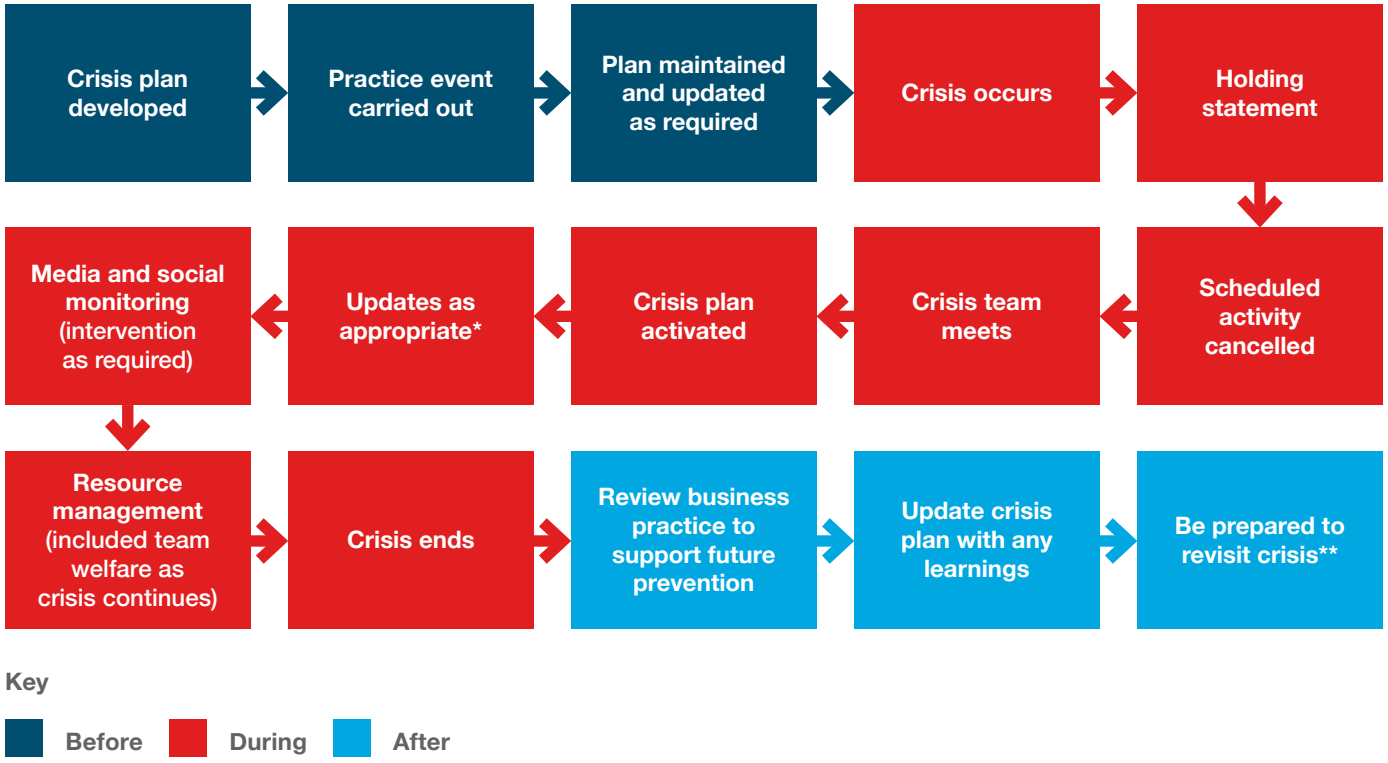
Crisis communications: a checklist

Insider events are generally assessed by their 'hard' organisational cost and financial impact over opportunity costs addressing cultural, reputational and relational aspects of your team.

In this respect, when it comes to insiders, ignore your people at your peril. They can prove to be both the source of your crisis and your front line for mitigation and defence. Taking a human-led approach throughout – before, during and after the event – will help increase your resilience.

When a crisis breaks, the timeline for action is very tight. Preparedness will be key.

The flowchart helps chart clear milestones no matter what form your insider crisis takes.



* People first, show empathy, be in control, internal and external audience.
** Victim and family support, staff welfare, outcomes of investigation, copycat incidents, anniversaries.

What the future holds

From NPSA

As this guidance goes to press, it is not a question of ‘if’ but ‘when’ a major insider incident will occur in the UK. It remains one of the largest yet unacknowledged security threats facing an organisation’s people today.

The nature of insider risk, where your people abuse their privileged levels of access, is changing. Increased recruitment by state-backed perpetrators, proliferation of digital access and macro-economic pressures on staff make it increasingly important to remain vigilant. The best approaches bring people inside the issue, helping them understand how they help detect and deter threat.

But research suggests we’re a long way from that. Today, there is no universal understanding of what an insider is, and only 40% of organisations have plans in place. What’s more, where plans exist, communication is often missing or generic in its focus.

Insider events demand a different approach from communication. Distinct to other crises, they surface organisational failure more explicitly, raising doubts around competency, culture or trust. They can be harder to detect and ideological-based motivations can be more difficult to oppose than rational arguments. Operationally, the relational impact, can be widespread, in some cases straining the very partnerships needed to effectively defend against the crisis.

This guidance will be widely circulated and is intended to provoke discussion and debate amongst both communication and security professionals.

This way, we hope that organisations can continue to evolve and adapt their approach based on industry best practice and latest learnings. Collaboration and curiosity are fundamental to the success of this work and, ultimately, the improved readiness of UK-based organisations for an insider event.

Whilst this guidance is intended to facilitate this, it is up to senior leaders representing both functions to make that collaboration work in practice.

NPSA will help organisations embed the guidance in communications practice by signposting advice and providing practical tools to help achieve this aim.

Whether you are a communications professional in-house or a consultant, we hope that you benefit from this new guidance as much as we have enjoyed researching and putting it together for our industries.

Our thanks go to the authors – Claire Spencer, Kate Hartley, Louise Watson, and contributors – Rod Cartwright, academics and practitioners who shared their experiences so invaluably with the Agfora and Plus4 research team. A summary of the key research themes is included in Annex 4.

Further reading

References

1. CERT National Insider Threat Center Carnegie Mellon Software Engineering Institute (2018) Common Sense Guide to Mitigating Insider Threats, Sixth Edition
2. Proofpoint (2022) Cost of Insider Threat Global Report
3. Ekran System (9 March 2022) Insider Threat Statistics 2022: Facts and Figures
4. Verizon (2022) Data Breach Investigations Report, 2009 to 2022
5. Ponemon Institute (2022) Cost of Insider Threats: Global Report, Proofpoint
6. Cybersecurity Insiders (2021) Insider Threat Report
7. Greitzer, FL., Moore, AP., Cappelli, DM., Andrews, DH., Carrol, LA., Hull, TD (2008), Combating the Insider Cyber Threat, IEEE Security & Privacy, 6 (1), 61–64
8. Hartley, Kate (2019), Communicate in a Crisis: Understand, Engage and Influence Consumer Behaviour to Maximise Brand Trust. London: Kogan Page
9. Schaufeli, W (2014) What is engagement? In Employee Engagement in Theory and Practice, C Truss, A Kerstin, R Delbridge, A Shantz and E Soane (eds). Abingdon, Oxon: Routledge
10. Bridger, E (2015) Employee Engagement. London: Kogan Page
11. Carlebach, E (2021) Exploring Public Relations and Management Communication. R Tench and S Waddington (eds). London: Pearson
12. Gillespie, N (2018) Six Ways to Rebuild Trust After A Crisis, University of Queensland Business School
13. NPSA (2022) The Insider Guide to Insider Risk. Media analysis of coverage on Insider Risk, 22 August 2013 to 11 August 2022 using Netbase QuidPro
14. National Crime Agency
15. Annual Fraud Indicator (2017)
16. 2019/20 Crime Survey for England and Wales (CSEW)
17. US Department of Justice Federal Bureau of Investigation (June 2018) A Study of the Pre-Attack Behaviours of Active Shooters in the United States between 2000 and 2013
18. CPNI and CIPR (2019) Crisis Management for Terrorist-Related Events

Annex 1

Crisis communications: a checklist

A crisis communication plan should be a core component of any organisation's risk preparations. Here are a checklist and guidance on what such a plan should include.

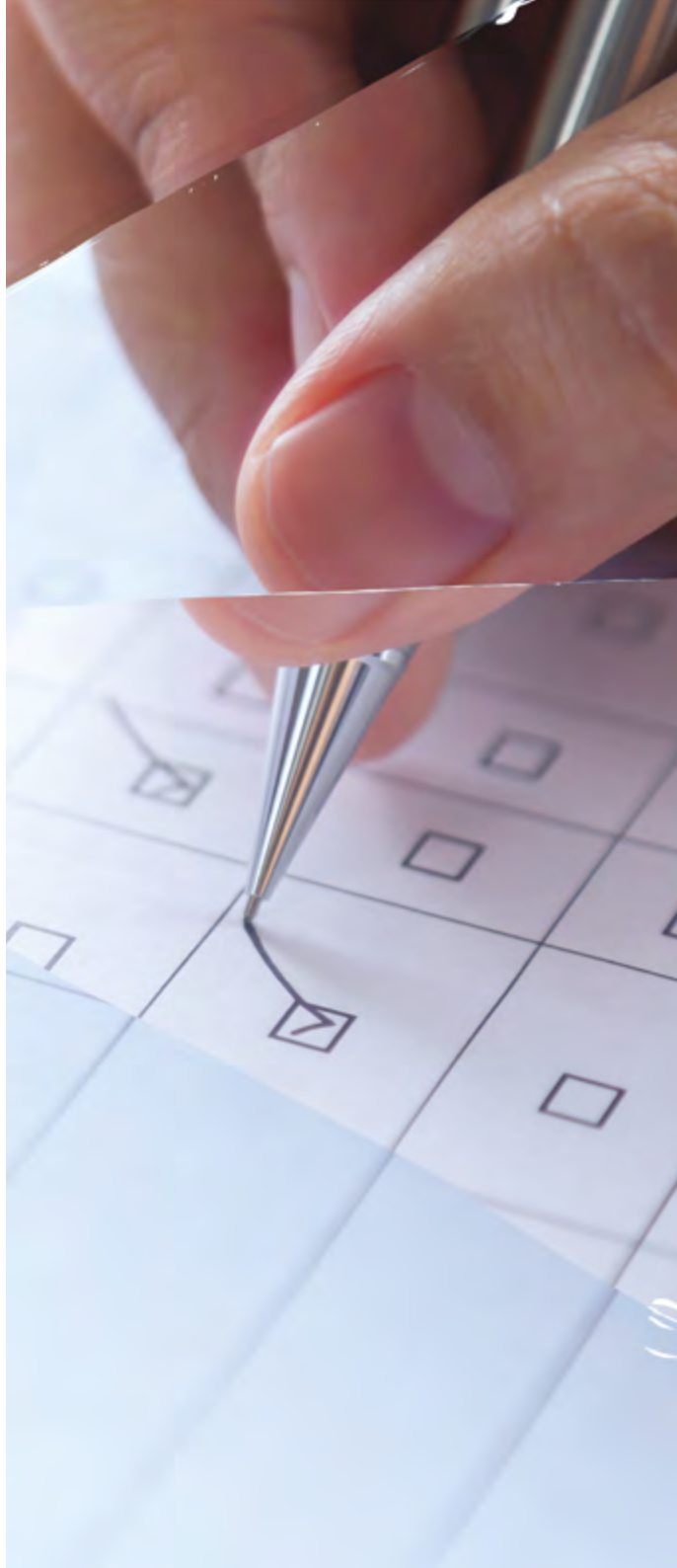
It should be developed following a detailed risk analysis looking at potential issues and possible solutions. Typically, these issues relate to an organisation's people, assets, property and operations, and the plan is there to guide action and communications.

When it comes to specific management of a crisis, here's a checklist of generic crisis best practice principles:[8]

- **Cast the crisis team.** It should involve those responsible for managing the crisis and communicating with internal and external audiences. Consider representatives from the leadership team, HR, legal, compliance and risk, internal communications, PR and communications, marketing, technology, IT, social media and customer service as well as any technical experts. Clearly define roles, including who is responsible for decision-making. Appoint decision-makers for each function and a deputy in case the lead is out of action. Agree who will be the crisis lead for different types of situation
- **Scenario planning.** Come up with every possible scenario you can think of that would negatively impact your organisation. Categorise by type and then by level of threat to the organisation. Many organisations choose to workshop this process to enable diversity of perspective. The document should be viewed as a living document, and other scenarios should be added as they are identified. You may structure your scenario plan by 1) Threat Level 2) Damage Potential 3) Example Scenarios in each case
- **Identify which crises could be avoided by business action.** Looking at each scenario in turn, what would it take to minimise their impact or avoid them altogether? As the nature of threat is always changing, learn from similar crises you or others in the industry have faced. Shore up your systems
- **Agree action for each level of crisis.** Define what normal looks like, what an issue looks like and what a full crisis looks like. Identify the metrics that would delineate an issue from a crisis. Next, define the appropriate level of action for each. That might include guidance on when to take no action but keep a watchful eye on an issue to monitor when it escalates
- **Develop your crisis plan.** A business continuity plan will take into account how the business will function – this addresses how you will communicate. This should be securely held and comply with relevant data regulation. (A suggested list of what your crisis plan should include is included on the next page.)
- **Streamline your approval process.** Speed is of the essence, keep everyone close who needs to approve a statement and, ideally, get as much as you can pre-approved
- **Train your team and simulate a crisis to rehearse them.** A crisis plan is all very well, but if your team doesn't know how to use it, it's useless. Hold regular (twice a year) training sessions on your plan (this will also enable you to critically review your plan and spot any gaps in it). Hold realistic simulations to rehearse a crisis, testing your plans and processes and building muscle memory in your teams
- **Revise and update your plans regularly** (at least annually) to make sure the information is up to date
- **Considerations.** Think about back-up plans. What happens if a member of your core team is ill or called away? Or the crisis breaks while they're on a plane? How will you communicate if your systems are down? Have a communication system that is secure and accessible off the corporate network

At its most basic, a crisis communication plan should include:

- **The contact details** of all your crisis team including back-ups in case individuals are out of reach
- **Clearly defined authority and a chain of command** including individual responsibilities and deputies
- **A clear activation plan and escalation process.** Every member of staff will know what unusual or concerning workplace behaviour looks like and who they should report it to. Have a team that is authorised to activate the plan. They should be part of the wider crisis team and accessible to anyone who might spot a crisis. Activation can be as simple as a telephone call to the crisis leader who can send a secure message to the crisis team, "We are in crisis level 2, plan activated". That process should include who can make the decision to wake the chief executive at three in the morning whilst on holiday
- **A defined decision-making process**
- **Out-of-hours access information.** To buildings, social media accounts, websites
- **A detailed action plan** for the first 24 hours of a major crisis
- **Approval processes and approved templates for statements to speed up approvals.** Include here guidance on how to personalise statements when you're responding publicly to people on social media. Your corporate media statement may not travel well on Facebook
- **Strategic intent statements and company values.** These make decision-making easier
- **Tone of voice guidelines.** Don't veer from your usual tone of voice during a crisis, becoming closed off, overly corporate or legal-sounding. This can be damaging. Give examples of words and phrases you can use publicly to avoid having to get every Tweet approved by a lawyer
- **Facts and figures.** Have business information to hand, like the number of staff at each location, where you operate in the world, your fleet size
- **Practical instructions.** This might include how to activate your crisis monitoring and social listening, how to contact your external agencies, how to access your social media accounts
- **Access to key external contacts.** Who is responsible for contacting each of them and at what stage of the crisis. They will include customers, investors, shareholders, workforce, partners, suppliers, agencies, contractors, media and influencers
- **Checklists of what should be done by when.** This means managing a crisis becomes following a process as much as possible, which removes significant stress from the crisis team



Annex 2

‘It’s OK to Say’

NPSA research has shown that unusual and concerning behaviour can be a precursor to an insider event, but an early intervention can result in preventing the act from happening.

The ‘It’s OK to Say’ programme is designed to encourage your organisation’s workforce to trust their instincts and take personal responsibility for staff welfare and security by intervening in a proportionate way if they witness unusual or concerning workplace behaviour.

The two parts of the ‘It’s OK to Say’ programme involve communications and training professionals working together for maximum impact and effectiveness.

Unusual or concerning behaviours can take a variety of forms, sometimes emerging in a change of usual behaviour. This is sometimes referred to as a person’s baseline behaviour.

These unusual or concerning behaviours fall into several categories.

- Behaviours that suggest potential individual vulnerability or risk. For example, changes in work-related attitudes and behaviours, signs of struggling with negative events resulting in significant anxiety and stress. Signs of addictions (gambling, alcohol, drugs), insecure behaviour on social media, inappropriate and aggressive behaviour in the workplace
- Unexpected or difficult to explain work activities that cause concern. For example, working unusual hours without a clear reason, exporting large quantities of data without a business justification, excessively seeking out sensitive information and knowledge not required for the role
- Work activities which are unauthorised. For example, using electronic devices where not permitted to do so, accessing unauthorised areas, unauthorised sharing of sensitive information with a third party
- The ‘It’s OK to Say’ programme contains editable materials for communications professionals to use as part of a security campaign, including posters, a video, an animation and digital communications for intranets

Annex 3

Insider crisis simulations

NPSA research reinforces the importance of real-time crisis simulations; however, there is no universal understanding of what an insider event is and the form that a crisis could take.

To address this, NPSA has partnered with crisis communications specialists to develop four insider crisis simulation scenarios. Each scenario is inspired by real-world reported events and creative licence has been applied.

The scenarios test a range of insider events including unauthorised disclosure, sabotage and violence. Each scenario has been designed to be customisable by issue and industry to ensure relevant appeal for private and public sector organisations, a range of sectors and possible topics. A detailed how-to guide for facilitators accompanies the scenarios.

The simulations can be managed in both high and low-technology formats, using either flash-card-style stimuli or using specialist technological platforms.

For those wishing to use the technological platform, a rate card of costs has been agreed.

The four insider scenarios include:

1. Unauthorised disclosure (activist based)
2. Unauthorised disclosure (state actor based)
3. Sabotage
4. Violence

Annex 4

Research findings

1. **Opportunity to increase insider knowledge.** Little universal understanding of insider events. Give communications the tools to feel confident on the subject and be part of the strategic discussion. Communication plays a role beyond limiting reputational damage. It can help educate, deter and reassure staff before and after an event occurs.
2. **Acknowledged need for communications support** 'upstream' before an insider event occurs. Communications play an important role in helping organisations to build a safe security culture, getting staff to engage with protocols and advice and encouraging staff to report any concerns.
3. **Reliance on generic crisis plans.** As it's not always possible to identify that an insider is the cause of an issue, many crisis communication plans are inevitably cause-agnostic, giving standardised advice for handling insider events in the same way as any other crisis event. Insider events do place more onus on internal communication and addressing issues of perceived fault.
4. **Managing roles and responsibilities.** Responsibility for different aspects of communication often sits across functions and, like with all crises, integration to break silos is important.
5. **Practice improves understanding, buy-in and confidence.** It's widely understood that a crisis plan is only as effective as the effort that goes into testing it in real-world situations. Running crisis simulations internally or through external partners was seen to be invaluable in building muscle memory, increasing confidence, raising buy-in amongst senior management and even improving outcomes. Conversely, research highlighted a lack of uniform understanding of how an insider incident could come to life, suggesting help is needed to bridge theory and practice.
6. **Communications clarity and consistency.** Whilst communication can increase vigilance, deterrence and leadership buy-in, there was a lack of consensus around how to deploy communication effectively in the case of an insider event. Research highlighted the need to agree clear and consistent messaging for both internal and external stakeholders and create a common language across functions.
7. **Focus on the outcomes not the people involved.** Clarify what can and cannot be shared, respect confidentiality and close down speculation. Research reinforced the need to fill the void with actions taken by senior leadership.
8. **Rebuilding relational trust.** Many who experienced an insider event described the destabilising effect that it had on their workforce. Communication plays an important role in recovering that trust after an event.

National Protective Security Authority