CPNI
Centre for the Protection of National Infrastructure

INVESTIGATING EMPLOYEES OF CONCERN
A GOOD PRACTICE GUIDE

MARCH 2011

Contents

Introduction

Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides advice on protecting the country's essential services, facilities and networks from terrorism and other threats.

The National Infrastructure

Nine different sectors form what is known as the national infrastructure. These provide the services which support everyday life.

They are:

- Communications
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Transport
- Water

CPNI provides security guidance, training and research from a physical, information and personnel security perspective. It aims specifically to reduce the vulnerabilities within these sectors, with particular emphasis on the most critical elements. Loss or disruption to any of these could cause severe economic or social consequences or even loss of life.

In addition to the nine sectors above, CPNI also provides similar advice to organisations engaged in planning and running the London 2012 Olympics.

The aim of this guidance

This document provides guidance to employers on the various stages involved in the investigation of employees of concern.

While some, typically larger, organisations have dedicated investigators and/or investigation teams, many do not and when concern is raised about an employee, organisations can be unsure of how to react, particularly if an accusation of wrongdoing is hard to prove. Furthermore, in some previous cases, employers have reacted disproportionately to such accusations and found themselves either in costly employment tribunals or with an unhappy workforce.

With the correct procedures in place, with employees who understand policies and regulations and with competent investigative personnel, organisations are better able to avoid potential legal pitfalls.

In writing this guidance, CPNI has consulted a range of bodies, including employers from the private sector, other government departments, law enforcement agencies and legal specialists.

CPNI recommends that organisations seek professional advice, especially on employment law, when implementing or amending their personnel security measures.

This document should be read in conjunction with other guidance published by CPNI, in particular:

- *Risk Assessment for Personnel Security: a guide*
- *Ongoing Personnel Security: a good practice guide*
- *Managing the disclosure of employee-related information*

Policies and procedures

Introduction

Many organisations will at some point need to carry out some kind of internal investigation into a member of staff. This could be for a wide range of reasons and, as will be described later in this guidance, may or may not involve the authorities. The primary duty for the investigator of these incidents is to establish the true facts and to be fair and objective when gathering evidence and when dealing with sources and the suspect. In the event of an employee taking their organisation to a tribunal, any hint of unfairness, lack of objectivity and thoroughness, or oppressive behaviour will severely undermine a case.

Clear policies

It is important that organisations periodically review their policies outlining how employees should behave in the workplace (such as not harassing or discriminating against colleagues) and the consequences of not following them. These should be in the terms and conditions of employment and may be reinforced during induction and supplemented by easily accessible information in a staff handbook or on a company intranet. All employees should be required to sign an agreement saying that they have read and understood the terms and conditions.

It is also important that the terms and conditions of employment should state the employee's responsibility for information security. Where appropriate, these should state that responsibilities are extended outside the organisation's premises and outside normal working hours, such as in the case of remote working. In some instances, these responsibilities could continue for a defined period after the end of the employment.

Not having these policies in place may make it harder to investigate and discipline staff suspected of wrongdoing, as their defence could be that they did not know better. An example of this is an Acceptable Use Policy (AUP) for staff email and internet usage. Each time a member of staff logs on to their computer, they have to acknowledge a prompt that outlines what they are and are not allowed to do. By clicking on this prompt, the employee will find it hard to argue that they were not aware they should not have been looking at say, an extremist or pornographic website.

Organisations are strongly encouraged to have an AUP[1] as without one, it is difficult to deal with employees who access offensive material in the workplace. Furthermore, if an employer does not enforce such a policy, they may find themselves at risk of complaints from their own employees. In one incident, an employment tribunal found that downloading and viewing pornography in the office by male workers constituted sexual harassment as it made the working environment unpleasant for a female co-worker, even though it was not directed at her.

Policies such as the AUP and terms and conditions need to be reviewed on a regular basis to ensure that they are appropriate, legal and proportionate.

[1] For more information on AUPs, please see www.businesslink.gov.uk/bdotg/action/detail?itemId=1076142205&type=RESOURCES

Disciplinary action

Employers should have an up-to-date disciplinary policy. Employees should be made aware of this and asked to sign, either manually or electronically, to say that they have read the policy. This should ensure correct, fair treatment for those who are suspected of wrongdoing.

Any procedure should be in line with the guidelines set out by the Advisory Conciliation & Arbitration Service (ACAS)[2] code of practice on discipline and grievance[3].

Investigations

Organisations need policies on how investigations are to be conducted. There should be step-by-step procedures, detailing how evidence should be collected and held during an investigation. These procedures should reflect what is required by corporate HR and security policies, as well as employment legislation.

A clear, straightforward list should help ensure a comprehensive investigation and record how and why investigators came to their eventual conclusion. This will be crucial should an investigation result in legal proceedings.

Who carries out investigations?

Some organisations will have dedicated investigators, while others may only have someone who does the job on an ad-hoc basis. These investigators may come from the security or HR departments or they may sit separately in their own section. This will depend on the nature of an organisation, its staffing levels and budgetary constraints.

The investigators should have a range of skills and be good at working with people. Ideally they will be trained in investigative techniques and interview skills[4].

It is also recommended that investigators make contact with their local police to find out what support can be offered. They may be able to offer advice on matters such as the kind of evidence that is needed to carry out a prosecution.

It is also worth keeping abreast of new trends in investigative practices. This can be achieved by attending forums, consulting lawyers, joining professional associations and reading relevant literature. In some sectors, investigators from different but similar companies may wish to meet to discuss relevant issues.

Raising awareness

Employees are advised to carry out regular security awareness campaigns, starting at employee induction and including refresher or bespoke courses. These campaigns should inform staff about whom to contact if they have any security concerns. By carrying out training, by explaining how security awareness is to everyone’s benefit and by presenting the investigatory personnel as approachable, staff are more likely to report security concerns.

[2] The official body dedicated to presenting and resolving employment disputes
[3] www.acas.org.uk/CHttpHandler.ashx?id=1047
[4] The Chartered Institute for Professional Development offers a range of interviewing and other related courses - www.cipd.co.uk

Having clearly defined policies and regular reminders about security will also have the benefit of improving the security culture[5] of an organisation. Employees with a better understanding of security issues and how these affect their organisation are more likely to follow procedures and report problems, and they are less likely to make unintentional errors themselves.

Management buy-in

All security measures need to be agreed upon and supported by senior management, with one senior manager having overall responsibility for security.

It is also appropriate to appoint a senior member of staff to provide oversight to individual investigations. This person will review the investigation as it progresses, redirect it if it goes beyond its scope or open up new avenues as necessary.

Ideally, the security officer should be independent of the business area which is under investigation. This introduces objectivity into the investigation.

Key points:

- Organisations need to have security policies drawn up and made accessible to all staff. These policies need to be read, understood and acknowledged.
- Policies need to be periodically reviewed.
- Investigators need to have the right skills and to keep abreast of current trends.
- Staff need to be informed about how and when they should communicate concerns.
- Senior management buy-in is critical.

[5] For more information on security culture, talk to a CPNI adviser or visit the CPNI website, in particular www.cpni.gov.uk/Docs/HYPERLINKED_OPS_May_2009.pdf

How employees come to be under suspicion

Introduction

It is important that organisations have a mechanism whereby employees can report suspicions about their colleagues. This does not mean that staff are expected to spy on one another, but when a genuine concern is felt, employees should know how to act on it. There is always a possibility that some malicious reporting will occur, but appropriate procedures and good investigators should help weed these out.

Line manager reporting

If an organisation has a security culture where employees are able to confide in their managers, they should be able to inform them of any concerns they may have about their colleagues, such as bullying, failure to adhere to security procedures, fraud or theft. This may take place at either regular meetings, security appraisals or on an ad-hoc basis.

Reporting hotlines

A hotline enables employees to report suspicions or actual incidents of illegal, unethical or improper conduct by their colleagues. It also provides a means for reporting suspicions about a colleague's behaviour. The hotline may even extend to providing a welfare function, helping employees who find themselves in financial difficulties, for example.

While 'hotline' is the generic term for an employee reporting facility, it need not be limited to (or even include) a telephone line, and could take the form of an internet contact site or dedicated company email address. Some organisations retain this capability in-house, while others outsource it to specialist firms.

In an organisation with a good security culture, the line manager will usually be the first point of contact for an employee who wishes to report unauthorised activity. Reporting hotlines are not designed to replace this relationship; they are intended to provide additional benefits such as anonymous or out-of-hours reporting, where this is desirable.

Additional information on reporting concerns can be found at:

- *Ongoing personnel security: a good practice guide*

Reporting hotlines can often be anonymous. When such reports are received, an employer may have concerns over the veracity of the information. However, taking efforts to determine the source's identity by attempting to confront a possible source can be counterproductive, while speculation on the source identity may jeopardise future source reporting, albeit anonymous. Guessing at the source identity can also lead to false trails and unsubstantiated information.

Instead, anonymous sources should be encouraged to come forward and provide their identity, especially when the information is significant and /or could lead to future prosecutions. This might include a recommendation to staff such that if they choose to remain anonymous, it may decrease the chances of being able to conclude an investigation, due to the inability to clarify matters.

Staff should be made aware that disciplinary action may result if reporting is found to be malicious.

Disclosures

In some instances, officials from security authorities such as CPNI, SOCA, UKBA or the police may wish to speak to an employer about a member of their staff. Typically this will be to request information about an employee to help an ongoing investigation. This may not necessarily mean the employee is engaged in any illegal activity; they may be linked tangentially to an investigation.

Additional information on disclosures and what to do should your organisation be contacted by a security authority can be found at:

- *Managing the disclosure of employee related information: a good practice guide for employers*

Other sources

As well as official reporting channels, there are a number of other ways where concerns about employees may be expressed. These have included canteen gossip, complaints from members of the public and acts of revenge by disgruntled friends or spouses.

Key points:

- Employers need to offer their staff easy to use, non-confrontational and secure means of registering concerns about colleagues.
- These measures need to be well advertised within an organisation.
- It is important for investigators to consider the motivation of the accuser before any action is taken.
- Anonymous and/or malicious reports are not uncommon. Organisations need to consider how they wish to deal with these.

Scope and purpose

First steps

Before any decision is made to explore an accusation against an employee, it is essential to have a plan outlining the investigating process. Some organisations call it a ‘scope and purpose’ document, others an ‘impact assessment’. The aim of the plan is to establish whether an investigation is actually necessary and to set out its boundaries.

An introductory statement need not be lengthy; it only needs to establish the reason for the investigation. For example, ‘This investigation is based upon a report that X disconnected system monitoring equipment and thereby caused a major shutdown of equipment resulting in disruption of critical systems’.

The statement should summarise the information which suggests the need for an investigation. It should do so in neutral terms which do not suggest that anyone has prejudged the issues. The statement helps start the investigation in a focused and impartial way.

It is also important that this document is signed off by management. Without such backing, investigations can potentially fail. Furthermore, it is possible an investigation may uncover issues senior management might rather avoid – such as the ignoring in the workplace of a particular legal requirement. Their involvement from the beginning will help reduce possible problems at a later stage.

Before beginning the actual investigation it is crucial that those responsible for its conduct are familiar with all the relevant policies and procedures related to or influenced by the investigation. They must know what should, or should not, have occurred and what the policies and regulations permit.

Key points:

- Some form of written guidance outlining the purpose of an investigation will help guide investigators through the process.
- Management buy-in from the beginning is essential in order to reduce potential repercussions at a later stage.

Factors to consider

Introduction

Employers need to consider a range of issues when embarking on an investigation. This will include whether an investigation is warranted and will consist of a conversation within the investigatory team and perhaps some exploratory questions to other relevant departments. Exploring these issues should ensure the investigation will be fair, proportionate and appropriate. For example, the following questions might be asked should there be concern about a member of staff seen working in the office at odd times of the day.

Is working late a normal situation?

- It is important to consider that the employee may in fact be doing nothing wrong and that due to the pressures of work needs to stay later in the day to meet a deadline or cover staff shortages.
- If there is a culture of working late in that office or department, the employee may simply be doing what others have done.
- Is the employee dealing with counterparts in different time zones, thereby necessitating unusual working hours?
- Is the employee working different shifts and starting later in the day, thereby needing to stay late?
- Has the employee done something like this before?
- Are they working alone or are there several people in the office?

Is the person simply not very good at their job?

- The employee may be staying later to catch up because they have been struggling with their work during normal office hours.

- **Is the person carrying out some sort of non-work related but legitimate/less serious activity?**
- The employee may be surfing (legitimate) internet websites or studying.
- The person may be moonlighting, using office resources for their own ends.

- **Does the employee have a reason for not wanting to leave work?**
- The employee may be having problems at home or elsewhere. The employee's personal circumstances may need to be considered.

- **Who reported the colleague?**
- It is possible that the person raising the issue may have a grievance against either their colleague or the organisation. Could the reporting actually be a malicious act?

- **Is the line manager putting pressure on the employee?**
- This may be legitimate pressure, such as the line manager being instructed to meet a deadline by their superior. Or, it may represent some form of bullying, intimidation or poor management.

Could an investigation damage the reputation of the organisation?

- It is possible that if details about the investigation, especially if the employee is suspected of doing something particularly serious, were released into the public domain, the reputation of the organisation may suffer.
- Organisations may also need to consider the issue of vicarious liability. Not only will the actual activity that the suspected employee is accused of need to be examined, but the level of training and supervision that the organisation delivered may need to be explored.

- **Upsetting other employees**
- Investigators should be mindful of the fact that the investigation may impact on other staff and morale, especially if the suspected employee is popular or seen as being picked upon.

- **Could there be a cost factor?**
- A protracted investigation or the suspension or removal of the employee from their post may have financial implications (but may still be cheaper than allowing an employee who presents a concern to continue their activities).
- The criticality or sensitivity of the project or work the employee may be involved in may need to be considered if it is impractical or undesirable to hire a replacement.

Key points:

- Before an investigation gets underway, investigators need to consider a range of issues which may impact upon their work, the suspect and the wider organisation.
- All of the above are factors to consider, but the wording of the policy is key. If an organisation operates a zero tolerance policy, then no matter how awkward it might be for the company, there is an obligation to investigate concerns.

The investigation

Planning

The first thing to consider when contemplating an investigation is the purpose and anticipated outcome. Why is the organisation considering conducting an investigation? As mentioned in the previous chapter, there are a number of factors to consider. Will a simple discreet desktop review or enquiry, which the staff member concerned will never be aware of, be sufficient? Is significantly more information needed? What will happen with the data once it is collected? These are the kind of questions that need to be considered before a full scale investigation is launched and should be outlined in the scope and purpose document.

Once the above questions have been considered and it is determined that the original information or suspicion is credible and there is a need for additional information regarding the threat or action, an investigative plan must be devised to ensure all of the appropriate steps are taken during the investigation.

Some organisations choose to give their investigations codenames or reference numbers in order to act as discreet shorthand when referring to their work to avoid reference to specific individuals.

It is important to remember that an investigation may also uncover information that needs to be referred to other departments, organisations or government entities. It is appropriate to seek out guidance from outside organisations at the onset should questions or issues arise that do not fall within the organisation's normal remit.

It is important to remember that the primary goal of the investigator is to be an impartial collector of facts and circumstances based upon the initial information. The investigation must be for the purposes of the organisation, not for personal vendettas among staff, and must be within the scope of the organisation's powers and responsibilities.

Investigators should always be mindful that in any investigation, unexpected developments may occur and the best laid plans, outlined in the scope and purpose document, may have to change.

In some very sensitive cases, legal departments have insisted on key personnel signing non-disclosure agreements covering before, during and after a case and stipulating that the specifics of an investigation can only be discussed with those who have signed the same agreements. As well as legal departments, a number of other individuals or specialists might need to be consulted during an investigation.

Information, documentation and evidence collection and preservation are an important part of any investigation. The usefulness of the investigation may be determined by how well the person conducting it documents and collects their findings. Well-organised notes, written statements (if available), photographs or videos, audio recordings and anything that substantiates or refutes the original accusation or suspicion is of vital importance and must be collected in a professional manner and in accordance with company policy and regulations.

Every effort should be made to ensure policies, regulations and applicable laws are followed during the conduct of the investigation.

Ending the investigation

Conclusions and recommendations based upon the information gathered should be provided to those members of the organisation who will decide what is to happen to the employee under suspicion (see page 28). Whether the observed behaviour or incident warrants company intervention or needs reporting outside the company, a concluding paragraph will pull together the information obtained in a brief summary of facts.

Key points:

- The scoping of the investigation should begin with defining why an investigation is appropriate and necessary.
- The planning process should include inputs from management, human resources, legal and other stakeholders with knowledge and insight into the issue or action.
- It is crucial that those responsible for the investigation be familiar with all the relevant organisational policies and procedures.
- Outside agencies, such as the police, may be consulted from the beginning in order to better understand any potentially difficult issues.

Whom to inform?

Introduction

There are a number of other individuals, departments or bodies that it may be desirable or indeed necessary for the investigator to consult or inform before, during or after an investigation. In some cases, only a handful of people outside the investigation team will be informed; in others, a wider circle will be needed. Either way, the decision on who else to inform should be taken carefully, so as to restrict the circle of knowledge and to reduce the chances of a leak.

Who should be consulted will vary as each investigation and organisation is different, but the following list should help employers when drawing up investigation protocols.

Line manager

Ideally this person should be best placed to evaluate what the employee was doing and why; whether there are any previous examples of unusual behaviour; whether the employee has had disagreements with colleagues and whether the behaviour is in any way unusual.

Of course it is possible that there may be suspicions about the line manager. They may be suspected of colluding with the employee or they may be thought to be putting some sort of unfair pressure on the employee. In these eventualities, a decision may be made to bypass the line manager and approach senior management directly.

Human resources

HR may have background information on the employee that may influence an investigation. They will also play a part should the outcome of the investigation affect the employment status of the employee in question.

Some organisations may outsource HR or, if the organisation is multi-national in nature, the employee may have been employed by an overseas office which operates under different legislation, and this may influence what information the investigator can access.

Security department

If the investigative team is separate from that of security, there may be calls to utilise help from the security department with matters such as manual searches.

IT department

If the employee is accessing unauthorised IT systems/websites or sending and receiving excessive or offensive emails, IT support will be required to carry out some form of audit of information. The IT department may also be in charge of controlling/monitoring access control.

Senior management

It will be necessary to inform senior management should the potential exist for adverse publicity or litigation for the organisation arising from the investigation.

Finance

If there are concerns that the employee may have been involved in any form of financial wrong-doing, the accounting or financial departments should be engaged.

Legal

It may be necessary to inform and take advice from internal legal counsel or the organisation's lawyers, should there be concerns over any legal issues.

Press office

If there is a risk that the investigation into the employee may result in media exposure, it would be prudent to have press lines prepared.

Trade unions

If the employee is a member of a trade union or if the employee has elected employee representatives, a decision may be taken to inform that union at some point in the investigation.

Law enforcement

If the employee has been identified as carrying out an illegal activity, it will be necessary to inform the police. However, it is not necessary for an organisation to stop investigating the employee, though direction may be suggested by the police. The police may ask for an investigation to be deferred, but it will be for the organisation to decide whether to do so.

Other official bodies

If the investigation into the employee and any assessment the employer undertakes in relation to the employee indicates that the person may be involved in an activity that is suspicious and may be related to terrorism, espionage or organised crime, but there are insufficient grounds to take action, a decision may be taken to inform other official bodies. These may include the police or CPNI. Employers should appreciate that authorities may not be able to provide definitive answers, only advice and guidance. The employer will need to make a final decision regarding their employee.

Other employers

If the employee is a contractor or on secondment, there will be a need to inform their employer either during or after the investigation.

The employee's colleagues

It is possible that colleagues may have to be spoken to at some point in the investigation, either as part of an evidence-gathering exercise or to inform them of how the investigation is proceeding. Once an investigation is completed, an employer may want to inform staff of the outcome. This may help to dispel any ill-informed rumours. Care must be taken, however, not to damage an employee's reputation.

Customers

If the organisation's employee is working as a contractor in/for another organisation, there may be a need to inform that organisation about potential compromises of their information.

Medical staff

If the organisation has a medical department and there are concerns about the employee's health or if their actions may have caused harm to others, it may be useful to speak to that department in order to gather relevant knowledge.

Key points:

- While each investigation will be different, it will be necessary for the investigator to consider the wider ramifications and who else might need to be informed.
- Investigators should be mindful of the fact that the number of people informed of the investigation should be limited to those who have a need to know. Any leaks may jeopardise the investigation or result in suspicions about potentially innocent employees.

Interviewing sources and suspects

Introduction

A key part of any investigation is the interviewing of sources and those under suspicion. Successful interviewers are well trained, non-judgmental and know not only what questions to ask and when, but how to listen effectively as well. Organisations such as ACAS or the Chartered Institute of Personnel & Development (CIPD) offer a range of investigative training courses.

Interviewing sources

A key aspect of an investigation is to interview the source of the original accusation. This may not be possible if the accusation has been made anonymously, but if the opportunity does arise, it may provide the investigator with useful background material. Moreover, if the source turns out to be biased and the accusation groundless, an interview will help avoid an unnecessary investigation.

One of the most crucial steps in conducting an effective investigative interview, whether of the source or suspect, is the clear identification of the interviewer to the interviewee. This will include an explanation of the accusation or suspicion, the purpose and process of the interview and whether the interviewee has anything to say before the interview starts.

Furthermore, the source should be informed that the employee under investigation has the right to know what they are being accused of and who made the allegation.

The investigator should ask the source why they provided the information and what, if anything, they expect from doing so. If the source's motive appears to be malicious it does not necessarily mean the information is unreliable, just that the investigator needs to treat it with caution.

During questioning, it is important to ask the source how they became aware of the information and if they know anyone else who might be able to assist with the investigation. The investigator should also establish whether the source has reported the matter elsewhere and whether they consent to their identity being revealed at a later date as part of the official investigation.

Source credibility

Determining confidence in the source can vary depending upon the level of cooperation given during the interview. It is also important to consider that a source's motivation may not be entirely pure. There is always the possibility that the source is providing information that is distorted, embellished or inaccurate. As a result, the source and the information that they provide may be difficult to evaluate at first. Further detailed corroboration may be required for a reasonable level of confidence in the source and the information to be established.

Documentation

It is appropriate to take notes while questioning the source and to produce a written statement of the interview. Ideally, the source should sign and date each page of the statement to

confirm its accuracy. Any amendments should be initialled by the source. Since most investigators do not have the power to execute a sworn statement, a written statement signed by the source will go a long way to providing confidence in the information.

It is easy for a source to make statements and allegations verbally. However, when asked to record any statement in writing, a source may refuse to do so or recant their previous statement. When this happens, the investigator needs to consider whether the information might be suspect or whether, by making the accusation official, the source is fearful of reprisals. The interviewer should be aware that the source may have been involved in the activity they are reporting, either as a witting or unwitting participant. If that is the case, special care must be taken to ensure that the source's right against self incrimination[6] is not violated.

As most organisations do not have the power to prosecute an employee, they do not need to abide by the tenets of the Police and Criminal Evidence Act 1984 (PACE) which lays out instructions on how a criminal interview should be conducted. Neither is there any need to make an audio recording of the interview.

If an organisation interviews a suspect employee who would have been cautioned in a police investigation, it may mean that the evidence is not inadmissible in a criminal court. However, this would not prevent the police using their own powers to interview the employee in any subsequent criminal proceedings.

More information on recording and reporting an interview can be found on page 27.

Source and information protection

At the end of the interview, the source should be advised that it is in their best interest to keep the information they have reported confidential at least until the conclusion of the investigation. The source should be given an assurance that they will be informed if any actions are taken based on their reporting. However, the source should also be cautioned about the privacy rights of the subject of the investigation and that they should not make the existence of the investigation or any of its details public. If the source reveals details of the interview or makes allegations against the subject of the investigation, they should be made aware that this may jeopardise the investigation and that breaching confidentiality could lead to disciplinary action.

Distinguishing facts from opinions and hearsay

Investigators often have to distinguish between fact, opinion and hearsay. Without the ability to distinguish between these types of statements, the information gathered may be less useful.

It is important to listen to the interviewee and determine if the person is making statements which they are offering as fact or opinion. Sometimes the investigator can accept a statement of fact as fact. However, most times it will be necessary to verify statements since they may be given as opinion.

Wherever possible, the investigator should try to gather facts. Opinion and hearsay are permissible in an employment tribunal but invariably colour proceedings. If they are presented, they should be noted as such and not as a fact.

[6] Also referred to as the right to silence. This is the protection given to a person during criminal proceedings from adverse consequences of remaining silent.

How to verify information

Information can be verified through obtaining further evidence from other witnesses, documents and data. The source's evidence should be checked, for example, against CCTV, electronic data and other sources.

It is worth reminding the source (or suspect) that there might be alternative ways to verify their facts, for example, by asking them whether they think the office CCTV would back up what they just said. This can be effective in making the interviewee realise that the investigator does not have to take their word.

Source evaluation

Following each interview, the source's credibility, motives and the information provided should be reviewed. Once an acceptable confidence level has been achieved, it is time to plan out the next steps of the investigation.

Interviewing suspects

The next step may be to talk to the employee under suspicion. Many of the practices, such as documenting and verifying information, will be applicable to suspects as well as sources.

Before conducting the interview it is important to outline what facts are known, what information needs clarification or corroboration and whether there are any inconsistencies.

It is useful to plan the interview in advance. However, as the interview progresses, the interviewer should not feel tied to these questions and should feel free to seek clarification on any new issues that may arise.

It is vital not to expect specific reactions from the interviewee. Preconceptions most often result in narrowing the focus of the interview and restricting the flow of information. Furthermore, if expectations are firmly set in advance, any new information or change of direction during the interview will be harder to handle.

Wherever possible, it is advisable for two people to conduct the interview - one to ask questions, the other to write down the answers. This will help minimise the risk of something being missed and to ensure that the suspect's responses are correctly recorded.

It is essential to remember that the purpose of the interview is to gather information, not to interrogate the suspect in a hostile manner. It is important to create an atmosphere which encourages openness and increases the likelihood of information being offered, although this does not mean that all information is of equal value. It is easier for an interviewer to become more forceful as the interview progresses, rather than become more 'friendly' after an aggressive start.

Employees should be offered the opportunity to have representation from a trade union official or a colleague to accompany them. An interviewer who does not offer the employee an opportunity for support may be later accused of pressurising the interviewee or not following correct procedures.

When a criminal investigation is taking place by the police, legal representation is required.

As with a source interview, the suspect should be offered the chance to sign and date each page of the written statement of an interview.

Key Points:

- It is important to determine what, if anything, a source expects by providing information and to consider that a source's motivation may not be entirely innocent.
- Confidence in the information provided by the source can be strengthened by corroborating facts with supervisors or other employees or reminding the source or suspect that their claims can be verified by means such as checking CCTV.
- It is easy for a source to make statements and allegations verbally. However, when they are asked to record their statement in writing they may refuse to do so or recant their previous statement.
- At the end of the interview a source should be advised that it is in their best interest to keep the information they have reported confidential at least until the conclusion of the investigation.
- Suspects should be interviewed in a similar fashion to sources. The interviewer should remember that their role is to collect information, not to try to extract a confession.

Methods of investigation

Introduction

It is important to remember that the investigation is not a criminal inquiry. It is an internal investigation into a potential breach of the employer's policy.

The burden of proof will be 'the balance of probabilities', i.e. that it is more likely than not that the employee has committed the disciplinary breach. This does not mean that once the investigation has been completed, the police cannot take the matter further.

Should an employee under investigation be suspended?

The organisation's policies and procedures will usually set out the grounds upon which an employee may be suspended. Suspension is not a disciplinary sanction; it is part of the investigation process. A decision will need to be made as to when the employee is told that they are under suspicion (this could either be at the planning phase of the investigation or, as later paragraphs will explain, when considering whether to have a covert investigation) but when that moment arises, a suspension may come into effect.

Suspension is usually considered necessary when the employee under suspicion may interfere with the witnesses of the investigation. It may not always be necessary: the employer may consider to restrict the employee's access to equipment, property or evidence in question or to move them into another role for the duration of the investigation.

If the employee is suspended, the employer should remember to remove their ID cards, access control, remote IT access and any other necessary materials.

Running the investigation overtly or covertly

Where an employee is under suspicion, the nature of the incident will dictate whether they should be made aware of the investigation or not. A number of factors will influence whether an investigation needs to be carried out covertly, including (but not limited to):

- Whether a suspicion or actual incident has been reported, and the varying degrees of additional evidence gathering each of these types of report will normally require;
- Whether the incident constitutes a sustained or continuing unauthorised act that needs to be monitored without alerting the perpetrator;
- Whether the investigation relates to a planned unauthorised act that has yet to take place;
- The nature of the incident or suspicion.

Before a decision is made to proceed with a covert investigation, it may be appropriate to consider whether it is proportionate to do so. Does the seriousness of the alleged wrongdoing justify the level of intrusion into the employee's privacy that will take place in the event of a covert investigation? A decision to proceed with a covert investigation must be signed off by senior management.

Evidence

The collection and collation of evidence is the backbone of any investigation. There are many ways to gather evidence, any combination of which might be appropriate according to the incident or suspicion being investigated. These include:

- Interviewing sources;
- Overt or covert surveillance of parties involved (although covert surveillance should only be used in exceptional circumstances);
- Forensic examination of office equipment used by the employee;
- Examination of audit trails, such as telephone call logs, created by the organisation's protective monitoring processes;
- Reviewing CCTV footage;
- Reviewing the employee's use of company credit cards.

When gathering evidence, organisations should bear in mind their legal obligations under the following legislation:

- **The Human Rights Act 1998**

In particular, organisations should bear in mind the importance of respecting employees' Article 8 right to private and family life. Organisations conducting an investigation which may involve the collection of information relating to an employee's private life should ensure that any resultant infringement of the right to privacy can be justified. This means that the amount and extent of evidence collected should be both necessary and proportionate in the context of the type of investigation being carried out and the nature of the incident or suspicion.

- **The Data Protection Act 1998 (DPA)**

The DPA regulates the way in which personal data (including that which is collected in the course of an investigation) can be gathered, retained, stored and destroyed. For example, the DPA allows personal data obtained during an investigation to be retained for as long as is necessary for the purposes of that investigation. The organisation would need to be able to justify, by reference to the nature of the incident or suspicion or the likelihood of appeal, for example, why continued retention of the data is necessary. Information collected for the purposes of an investigation should normally be held for the duration of the investigation, as well as any time allowed afterwards for internal and external appeal processes.

- **The Regulation of Investigatory Powers Act 2000 (RIPA)**

RIPA legislates for using certain methods of surveillance and information gathering (for example, the interception of telephone calls or emails, and covert surveillance). It sets out legal requirements which must be followed if these types of methods are to be employed in an investigation.

In a criminal case, the investigator needs a system for logging evidence that is gathered. This log needs to provide an audit trail of movement of the evidence during the course of the investigation. These exhibits should be bagged and sealed and given a unique number. When showing these items to an interviewee the description and label number needs to be documented in the interview record. This applies to interviews of sources and suspects.

This level of thoroughness is not strictly necessary for an internal investigation. However, it is good practice and may assist an employer's case during any subsequent legal proceedings.

Investigations may need security of their own. Organisations should ensure that evidence is stored in a way which guarantees its integrity both for the duration of the investigation and for any additional time allowed for appeals and legal challenges after the investigation has concluded.

Searching

An investigator should usually be allowed to search locations or property belonging to their organisation. This includes offices, vehicles, computers, desks and company storage lockers. It is advisable to have a proviso indicating that this might be necessary in the organisation's security policies.

However, a bodily search of an employee, without express consent, will amount to an assault. Where it is imperative that such a search be carried out because there is strong evidence that the employee might be hiding a stolen document or have an article that could be used to harm others, then the police should be called immediately.

The timing of the search (of locations or property) and who is present should be done in coordination with company legal and HR representatives. Every effort should be taken not to advertise the fact the search is about to take place and when it does, efforts should be made to cause as little disruption as possible. In some cases, searches are best conducted in the presence of the person concerned and they should be done by someone who is specially trained and in a way that will not allow the person to destroy or hide evidence.

If possible, an independent person (such as a member of HR) should be present, who can observe the search and make note of anything that is removed, especially in the case of personal items. Another safeguard that may be appropriate and should be considered is photographing or videotaping the search itself, noting what is found and where. This will provide an easy way to document the search and serve as a record of the search process. In any case, a complete inventory of items removed from the search must be completed and should be signed by any witnesses to the search.

The investigator should try to gain access to keys that are needed for any relevant drawers, desks, containers, rooms or areas that need to be searched. If the keys are not available, make sure to get prior written approval to break into the container or area.

Finally, if evidence is found, the suspect should be asked about it and their replies noted as part of their statement.

While it may not directly be part of an investigation, if adequate notices and warning is given, it may be possible to institute a programme to inspect bags and personal property when individuals enter or leave a site. This sometimes happens in the retail and manufacturing sectors. Close coordination with legal and HR departments should be effected prior to implementing such inspection regimes.

It is important to get legal guidance on what may and may not be inspected in employee's possession and to specifically request authority to 'inspect,' not search personal property. It is also necessary to furnish a comprehensive justification for such inspections. By having such a programme in place, it may assist in future investigations if an employee is accused of removing materials from a site.

Monitoring

Monitoring is when an organisation carries out systematic or occasional checks on some of its employees. During an investigation, many of the methods of evidence gathering available to an organisation, such as opening an employee's emails, checking telephone logs and checking logs of websites visited by an employee, will amount to monitoring. There are particular issues to bear in mind in the context of an investigation, and the advice of a specialist in employment law is essential.

Whenever a form of monitoring is proposed as part of an investigation, organisations should reference section 3 of the Employment Practices Code[7] (the Code), which is issued by the Information Commissioner. The Code sets out recommendations in order to help organisations comply with the law when carrying out monitoring. For example, unless exceptional circumstances apply, such as where a covert investigation can be justified, employees should be made aware that they may be monitored.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the LBP Regulations) outline that an employer retains the right to carry out monitoring notwithstanding that the employee has not given their express consent provided such monitoring is necessary to carry out the following:

- Recording evidence of business transactions;
- Ensuring compliance with regulatory or self-regulatory guidelines;
- Maintaining the effective operation of the employer's systems (such as preventing viruses);
- Monitoring standards of training;
- Preventing or detecting criminal activity;
- Preventing the unauthorised use of the computer/telephone system – ensuring the employee does not breach the employer's email, internet or telephone policies.

Nonetheless the LBP Regulations and the Code stipulate that it is necessary for an employer to take reasonable steps to inform employees in advance that their communications might be intercepted and how the information obtained from the monitoring may be used. AUPs have already been mentioned (see *Policies and procedures*), but other methods may include periodic communications to employees, some form of training or the inclusion in employment contracts of information about certain types of monitoring.

Covert monitoring is only likely to be justified when the organisation has good reasons to suspect a criminal offence or other offence of a similar severity and will often be a last resort.

[7] www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf

The Code states that before commencing any monitoring, an organisation should carry out an impact assessment in order to ascertain whether the benefits which are likely to arise from the monitoring outweigh the level of intrusion into the privacy of the individual. The Code sets out relevant considerations to take into account when carrying out an impact assessment. Ideally, the process of carrying out an impact assessment should be documented.

The interception of emails is a form of data-processing and therefore the employer must consider whether the monitoring intrudes unnecessarily on the employee's privacy. The Code suggests that employers should:

- Actively consider whether the risk which any given method of monitoring is designed to address justifies that level of intrusion into the individual's privacy;
- Limit monitoring to traffic data rather than the contents of specific communications;
- Undertake spot-checks rather than continuous monitoring;
- As far as possible automate the monitoring so as to reduce the extent to which extraneous information is made available to any person other than the parties to a communication;
- Target monitoring on areas of the highest risk.

The Code also provides criteria which employers are expected to meet in order to comply with the Data Protection Act. It is apparent that in any prosecution or other enforcement proceedings, account will be taken of the employer's regard for these particular benchmarks and the first benchmark for employers is to: 'establish, document and communicate a policy on the use of electronic communication systems.'

Investigators should not accept tapes of conversations from employees or other people who may be trying to assist in the investigation. These individuals must be advised that it might be illegal for them to record such conversations. They should be asked to explain why they took the decision to carry out the taping. Legal departments should be immediately contacted for advice on what to do with any such recordings.

International differences

Multi-national employers should be mindful of the fact that different countries have differing approaches towards the extent that an employer may monitor employees. For example, European Union nations generally err on the side of the employee whereas United States law favours the employer. In another instance, a multi-national company may move staff from one country to another while servers might be based in a third nation. Different laws might apply for the host country, the foreign staff and where the servers are based.

More information on understanding a range of international issues can be found on the CPNI website. For example:

Overseas criminal record checks:

- www.cpni.gov.uk/*ProtectingYourAssets*/overseas.aspx

Personnel security in offshore locations:

- www.cpni.gov.uk/Docs/personnel-security-offshore.pdf

Reviewing progress

It is advisable to carry out periodic reviews as the investigation proceeds. Typical enquiries/investigations will relate to frauds, theft, sabotage or IT abuses where the company is the sole or main victim. These cases are not likely to interest the police until the bulk of the work is done (more on consulting with the police can be found on page 36). It is therefore recommended that within these periodic reviews, it is considered whether there is enough evidence to approach the police with a view of them taking over the investigation. An early approach to the police ascertaining what they would require to commence an investigation could prove useful to both parties.

Legal privilege

The employer should remember that legal privilege attaches to all communications between them and their legal advisers. Communications can not be disclosed without the permission of the client. The privilege is that of the client and not of the lawyer.

The investigative report and all correspondence and communications will not be privileged and will have to be disclosed and be subject to examination by a court. The same applies for notes, photographs and other documents collected or used in an investigation.

Key Points:

- A physical search may only be appropriate if there is reason to believe that information or evidence may be destroyed or lost.
- The timing of the search and who is present should be done in coordination with company legal and human resources representatives.
- Try to have an independent person present, who can observe the search and make note of anything that is removed during the search.
- Do not advertise the proposal to search and try to cause as little disruption as possible
- If it decided that monitoring is needed, it must be done legally and in line with the organisation’s own policies. The more intrusive the monitoring; the greater the justification.
- It is important to obtain professional legal advice.

Recording and reporting

Recording

Every stage of the investigation needs to be recorded in writing. This will include each step of an investigation – whether it is the original accusation, interview, the gathering of evidence, any delays and the outcome.

Report writing should be as concise and factual as possible and only present the information obtained during the investigation. The first paragraph of a report should summarise why the investigation was conducted and what company policies were suspected of being broken. It should present information and facts obtained during the investigation in a clearly understandable manner.

Reports may contain the personal opinion of the individuals interviewed or the original source (of the accusation), however, such opinions must be identified as opinions provided by the person being interviewed so as to not allow the reader to confuse them as facts. As an example, 'It is Mary's opinion that John's actions were completely inappropriate and hurtful in nature and were done only to anger his co-workers'.

It is preferable that investigators do not make formal findings of fact or apportion blame. Their role is to present the fact and to allow the reader, (the person who makes the decision regarding the employee) decide. Doing this will require discipline on the part of the investigator in order to ensure their findings are not in any way prejudiced.

The use of photographs, charts, diagrams and other depictions may be appropriate in the report of inquiry to illustrate or clarify details of the investigation or actions. Documents obtained during the investigation should be copied if possible and the original secured and maintained in an original state and made available for future actions. Any items which could be of future evidential value should be secured by the person who obtained them or turned over to appropriate authorities as appropriate.

It is possible that the report may be critical if the employee takes the employer to employment tribunal. If the company investigation has been fair and proportionate, demonstrating every step of the process, explaining why decisions were made and listing communications between the investigative department and their counterparts, then this may help those presiding over the case to make a decision in the employer's favour.

Key Points:

- The usefulness of the investigation may be determined by how well the investigator documents their findings.
- There should be expectation that the investigation will be completed in a timely manner without unnecessary delay.

Outcomes

Dealing with the employee

While the scope and purpose document will have outlined the aims and objectives of the investigation, the actual outcome may be harder to predict. Therefore, it may be worthwhile to consider possible outcomes in advance and how they may be addressed.

No action

- The suspicion may be dismissed as the investigation may find no evidence of wrongdoing.

Words of advice

- All that may be required is for the line manager to speak to the employee, pointing out any transgressions they may have made.
- If the investigation discovers that the employee is experiencing problems outside of work (or even at work, such as lack of confidence) there may be a need for words of advice.

Action against line manager

- If the line manager is found to be at fault, action may need to be taken against them.

Training for the employee

- The employee may need additional training to manage their workload/timekeeping in a more efficient fashion; to become more proficient in their area of work or learn more about the organisation's working practices.

Reassigning the employee

- If the employee has committed an offence which while serious, does not warrant their dismissal and it is decided they deserve another chance, there may be cause to move them to a different project or department. However, this will depend on business needs.
- Coupled with this reassignment, there may be a need to alter IT/physical access or remove security privileges.

Disciplinary procedures

Depending on the outcome and the appetite for dismissal, disciplinary procedures for the employee may be invoked. These must be proportionate to the offence and in accordance with the organisation's policies. The employee may be the only person who can do a particular task and if the offence is not deemed that serious, there may be opposition to reassigning them.

Dismissal

If the employee has committed a serious offence, a decision may be made to dismiss them. Such a decision will need to be in accordance with the organisation's policies. If the employee is dismissed, full and proper exit procedures should be followed, including ensuring physical and electronic access is revoked.

Whatever the reason for a dismissal, it is crucial that an organisation has disciplinary and dismissal procedures in place to deal with any eventuality. If these do not exist, an employment tribunal may rule against an employer.

More information on handling disciplinary and dismissal issues can be found in the ACAS guidance *Disciplinary and Grievance Procedures*[8].

It is likely that employees will face allegations of unlawful discrimination. Employers should note that the Equality Act 2010 allows employment tribunals to make recommendations in discrimination cases in respect of the employer's entire workforce, and not just the individual who has brought the claim.

For example, a tribunal may direct that an employer introduces or reviews an equal opportunities policy or delivers training to employees. Although an employer will not face any sanction for failing to comply with a recommendation of the employment tribunal which does not relate specifically to the claimant, such failure could be used as evidence against the employer in any subsequent claim.

Informing the authorities

At some point during an investigation, an employer may believe it necessary to contact the authorities (such as the police or CPNI) about their employee. If it is clear that illegal activity has taken place, this will not be a difficult decision to make and the police should be called. Indeed, if the general public is at risk of serious crime, not telling the police may damage the company’s reputation or possibly incur criminal liability

That may be seen as an attempt to pervert the course of justice or amount to an offence of impeding another’s apprehension or prosecution contrary to Section 4(3) of the Criminal Law Act 1967. There is also a positive duty to report certain terrorist activity under section 19 of the Terrorism Act 2000.

If the concern is less obvious and there is a belief that an employee may be linked in some way to terrorism or extremism, an organisation should contact CPNI. When this happens, CPNI may pass this information to the relevant investigatory bodies, which will then examine the information. CPNI may be able to return to the employer with some information about the employee. However, employers should appreciate that it may take some time for an investigation into the employee to result in anything conclusive, if at all, and there may be limits on what CPNI can tell the employer.

When a suspicion has been raised about an employee that is more difficult to quantify, the decision of when or even whether to inform the authorities is a more difficult one. It is impossible to define the exact moment of when an employer should take their concerns to an authority, as each case will be different. Instead, an employer needs to use their own judgement and consider the strength of a suspicion or accusation before they take them forwards.

[8] www.acas.org.uk/CHttpHandler.ashx?id=1043

Informing regulators

If the organisation for which the employee works is regulated, it may be necessary or a requirement to inform the regulator of the situation. If the activities of the employee affect other organisations within that sector, the regulator may need to consider introducing new measures to counter them.

Repercussions for the employer

While there are various outcomes for the employee, it should not be forgotten that the employer can also be affected by the investigation. Once the suspicion has been resolved, the employer may need to implement any of the following:

- If the employee is disciplined or dismissed, it is possible they will take legal action against the employer. This is why it is imperative that the correct dismissal/disciplinary procedures are followed by the employer.
- New training may need to be implemented to enforce the new procedures.
- Additional security measures may need to be put in place, such as access control.
- New IT monitoring/audit procedures may need to be enacted.
- New security culture implemented (along with the appropriate training) so that staff are more confident and able to challenge suspected wrong-doing in the work place.
- If colleagues feel that the employee has been badly treated, it is possible that this may result in resentment against the employer. This may manifest itself in a number of ways from poor staff morale through to industrial action.
- Adverse publicity about the employee and employer is unlikely to be welcome. If the employer fears that this may be the case, they should prepare statements for their dealings with the media.
- Possible action against the employer, especially by the police, in certain cases, such as money laundering.

Root cause analysis

As soon as possible following an investigation, a committee of stakeholders should assemble to identify what went right and what could be improved in the future. A review of policies and procedures should also be conducted.

The results of the post-investigative review should be documented and provided to senior management and any other relevant persons. This report should describe the actions taken during the investigation, and problems that arose and recommendations on how to improve future responses. Since this reporting may contain the identification of systemic or operational vulnerabilities, the dissemination of the report should be limited to those with a need to know the information.

Key points:

- In some cases, it may be difficult to anticipate the outcome of an investigation. While the investigator is unlikely to decide what action to take against the employee, employers should prepare for a number of different eventualities.
- Employers should also anticipate that the investigation may have some kind of repercussion for their business.
- A review of policies and procedures should be conducted to determine how well, and if they were followed during the investigation and whether updates or changes are appropriate.

Appendix 1: Investigative checklist

Step	Action	Complete
1	Does your organisation have security policies, available to all members of staff, which clearly stipulate what constitutes improper behaviour in the workplace, and what sanctions will be invoked if employees contravene these policies?	
2	Do employees have the means to communicate concerns about their colleagues?	
3	Have you prepared a scope and purpose document?	
4	Have you considered what factors may impact upon the investigation?	
5	Whom do you need to inform?	
6	Have you carried out the necessary preparation, including interview training, briefing the employee and preparing facilities to carry out an interview?	
7	Are you aware of the legal framework surrounding investigations?	
8	Is there a clear record of each step you take?	
9	If you are carrying out monitoring, are you doing so legally?	
10	Have you prepared a concise, factual report, to allow others to make a decision regarding the suspect?	
11	Once the investigation is over, is there scope for root cause analysis?	

Appendix 2: Incident response guidance – an exercise

This case study takes the reader through a fictional incident at a Critical National Infrastructure site. It may be reproduced and used in training exercises.

The situation

Based in the head office, you are the senior security manager for a large utility firm within the Critical National Infrastructure.

The report

Your 24-hour maintenance watch centre received a call from an employee, working at a key site, who reported that he had found a security survey report. The employee has said that the report contains vital information about the security measures around your site. The document apparently bears your company logo and proprietary markings reflecting that the document is ‘company confidential’ and is to be accessed only by authorised representatives of your company.

The response

Initially, it is important to make contact with the employee to obtain their contact details and to establish whether he secured the document. Once the status of the report is known, arrangements should be made to recover the document and interview the employee.

Source interview

Since this source appears to be cooperative and may have little reason to distort facts of the circumstances in which he found the document, you may want to consider an initial telephone interview with him, especially if he is off duty or in a distant location. Regardless of how the interview is conducted, the Five Ws (who, what, where, when, why) and how he found the document should be covered.

It is important to ask the source whether he knows who could have left the document unsecured. You should also advise him that it may be necessary for you or others to contact him in the future and conduct a more thorough interview as part of the investigation into how the document was left unsecured. It is also important to determine (i) if others may have come in contact with the document and (ii) their identity and contact information.

Outside considerations

Although the document in this case does not contain any government protectively marked information, the proprietary information in the document could allow interference of the workings of the key site which would affect a variety of commercial and government customers. It would be prudent at this point to contact a CPNI representative or other government agency as appropriate informing them of the circumstances, your actions at this time and the possible repercussions if this document were to fall into the hands of someone intent on causing harm.

Notification, policy, regulations and legal considerations

Once the basic details of the incident are known, your company officials, including your supervisor, should be briefed and given an indication of what actions you have taken and

where you are heading with your investigation. As appropriate, company policy and regulations, as well as legal staff should be consulted to ensure you are proceeding in a proper manner. With this guidance in hand, it is time to begin the investigation.

The investigation

The investigation should proceed along logical lines; be conducted in accordance with guidance obtained above; begin with interviews of those who would logically have normal control of the document and progress to determine the circumstances surrounding the document becoming unsecured.

Consideration should be given to the fact that the document may have been stolen by an unauthorised person who had access to the site, but who would not normally have access to the report. In this case, you will need a full-scale investigation rather than an administrative review, focused to determine if policies and procedures were ignored. The fundamentals of the investigation will change at this point and immediate contact with CPNI or a responsible government official should be made to relay the suspicion that the perpetrator may have purposeful intent to cause harm. This coordination should occur as soon as there is any indication that the incident has national security implications.

Post investigation recommendations

Based upon the findings of the investigation, a variety of recommendations may be made and should be forwarded to company officials who are responsible for issues discovered during the investigation. If policy and regulations were violated and documented in the investigative report, those responsible for the administrative controls must be notified. Should there be a breach of any laws by your employee, or the perpetrator if it is determined that an ‘outsider’ was involved, external officials must be notified. Since there is a multitude of possible outcomes from the investigation, company legal staff should be consulted before, during and at the conclusion of the investigation to ensure proper actions are taken as a result of the incident.

Corrective actions taken

The results of the investigation and the above recommendations will provide an opportunity to correct, modify or update company policy, regulations and procedures to make sure that the vulnerability that allowed this incident to occur has been eliminated. If the incident was a result of ‘insider’ actions, then it is vitally important to involve senior management, HR, legal staff and those responsible for the employee (line managers), as well as those responsible for the security of the document in order to review the incident, its impact on the company and establish future processes to prevent re-occurrence.