Dawn-raid ready

Mitigating the reputational consequences of a dawn raid

THE EUROPEAN Commission's security seals are made of plastic film. If they are removed, breached or otherwise tampered with, they do not tear, but show 'VOID' markings that then remain irreversibly visible on their surface. Would your company pay €38 million for a broken seal? How could a plastic seal possibly cost that much? €38 million is exactly what it cost energy company E.ON in fines alone, following a dawn raid on their premises in May 2006. The case was to go on until 2012 and saw the full fine upheld in court.

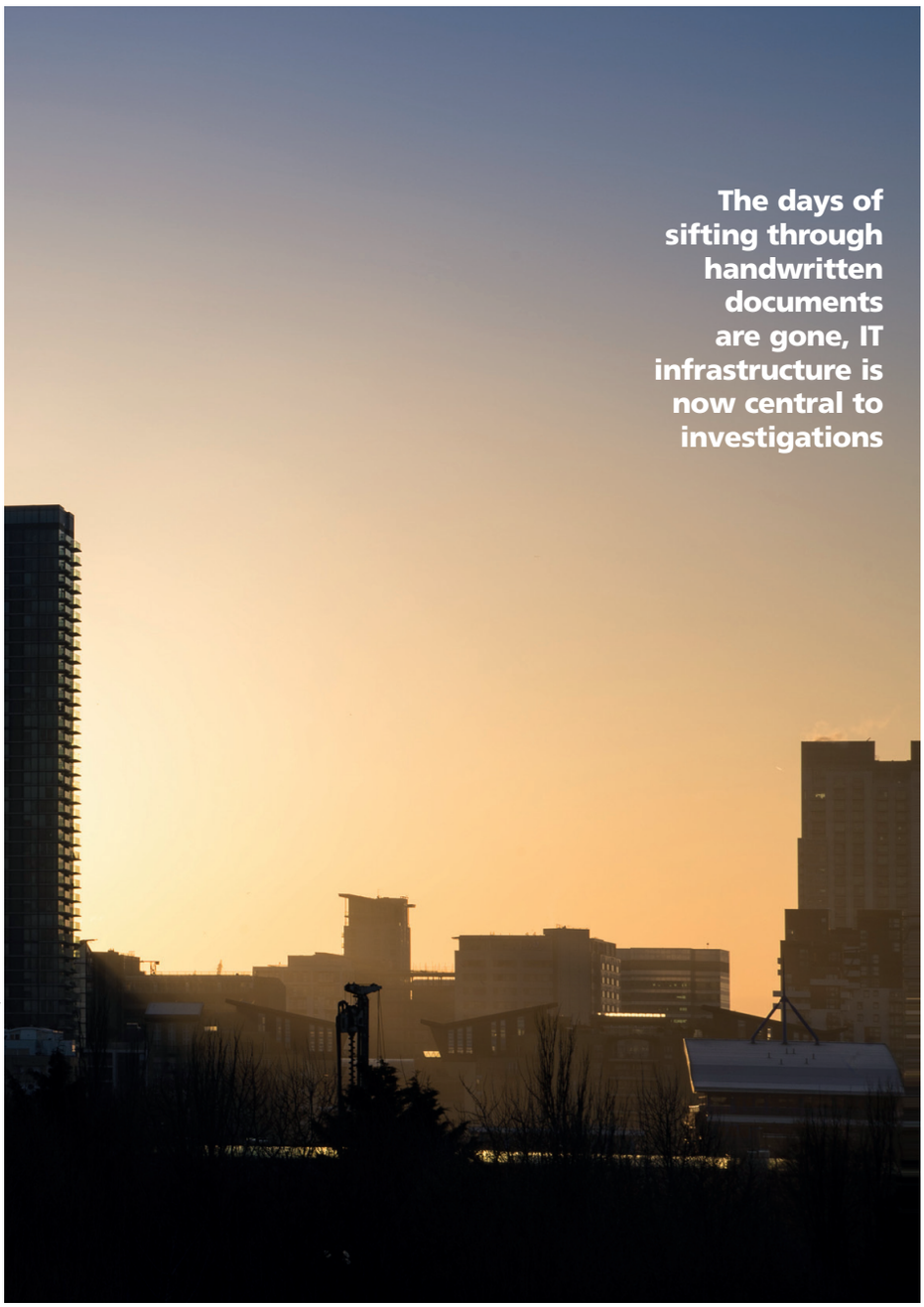
The European Commission (EC) concluded that E.ON or 'persons within E.ON's sphere of influence' had broken the seal, which had been placed on a nominated office door to secure seized documents. The EC was not in a position to prove conclusively whether the breach of the seal had been intentional or whether any documents were missing. It assumed that the breach of the seal had occurred, at the very least, as the result of negligence – since it was the responsibility of E.ON to ensure that the seal was not broken. In this respect, the EC noted that E.ON had not advised everyone authorised to enter the building – including the cleaner – about the existence of the seal and the need to respect it.

The raid was undertaken as a result of information received claiming that the E.ON Group was involved in anti-competitive practices within the European energy industry. In an ironic twist, after multiple court appearances, a €38 million fine and substantial costs, E.ON was not found to be involved in anti-competitive practices – which was the original reason for the investigation.

Subsequent developments

In March 2013 the EC published revised guidance on dawn raids. This guidance is, essentially, codification of custom and practice. Crucially it reflects recent developments where electronic company records predominate, rather than paper.

This revised guidance reflects the E.ON seals decision above, together with two other cases: EPH,



The days of sifting through handwritten documents are gone, IT infrastructure is now central to investigations

MATT GIBSON/SHUTTERSTOCK.COM

a Central European energy group (and others), and Koninklijke Wegenbouw Stevin (KWS), a Netherlands-based road construction company.

In the EPH case, the company changed a password set by the inspectors to regain access to an e-mail account that had been blocked as part of the dawn raid. This also diverted e-mails away from scrutiny. Consequently, the guidance now stipulates that companies must assist with investigations, particularly in relation to IT and systems. This assistance extends as far as IT experts being available to support access and provide temporary blocking.

The days of sifting through handwritten documents and filing cabinets are, to a degree, gone. A company's IT infrastructure is now central to investigations, which is deemed to include servers, cloud storage, PC's, mobile phones, iPads, USB sticks, DVDs etc. The Commission is also likely to regard any devices or data storage on the company's premises to be within scope, even if they are the personal property of employees.

In the KWS case, although the guidance recognises a company's legal rights to legal representation and consultation, the absence of such legal support does not render the inspection invalid. The guidance also specifies that companies can only prevent inspectors from entering their premises for a short period. This is critical for companies headquartered in major commuter cities – KWS's delay of just 45 minutes resulted in a 10% increase in their fine.

These principles are being more widely enforced. For example, the Polish competition authority recently imposed a €33 million fine on Polkomtel, the mobile phone network operator, for denying access to a hard drive. The Spanish competition authority imposed fines of €2 million on two ferry companies after a 45-minute unexplained interruption to the IT service during a dawn raid. Failures to co-operate more generally are also being enforced; a company received a €30 million fine for delaying the start of a dawn raid by over an hour. The inspection team was apparently waiting in reception while a meeting was held about how the raid should be managed. In practice, inspectors will now only be prepared to wait 15 to 30 minutes and will only do that if they are able to occupy areas of interest to minimise the risk of document destruction.

What are dawn raids?

Dawn raids take their name from the inspectors' usual approach of arriving at dawn, when companies are least likely to be ready for the unexpected. It also affords the inspectors the opportunity to secure documents, IT, offices, locations and other material considered relevant to their investigations. As a consequence, it is imperative that a company's dawn raid processes reflect reality – that a raid might take place at dawn. The only people available might be security officers who could have little familiarity with the company and who may not even be employees. Senior managers and legal officers could be 90 minutes or more away by the time they have made the commute. In any review of dawn raid processes it is essential not to lose sight of the practicalities.

The practicalities

The decision to review your company's dawn raid processes may have been triggered by a range of factors, including: concerns at the senior level, a dawn raid on a similar organisation, or a periodic corporate governance process review. The review team should be drawn from a range of key stakeholders, which is likely to comprise a core team of in-house lawyers and external competition and regulatory lawyer(s), compliance and training departments, auditors, HR, IT, corporate governance and process managers and building/security managers. Media relations, procurement, sales, marketing and retail operations should also be included in the team. The media relations team would ensure that, if appropriate, a press release is prepared as part of a dawn raid response pack. These individuals will also need to be available to deal with what could be significant media

interest. Procurement, sales, marketing and retail operations are also included as typical high-risk groups that could be the focus of a dawn raid, particularly where it involves suspected price-fixing, restrictive agreements, cartels, abuse of dominance and other anti-competitive activities. It is essential that the review team identifies the key dawn raid-related issues and how they apply in the jurisdiction(s) in which the company operates. These issues will form the basis of a dawn raid response plan.

Key issues

The first key issue would be the type of dawn raid and which agency could carry it out. In the UK, these agencies include – but are not limited to – the Financial Conduct Authority (FCA), HM Revenue and Customs (HMRC), the European Commission (in conjunction with the UK authorities), Serious Fraud Office (SFO) and the Competition and Markets Authority (CMA). Related to this is the inspectors' possible powers of investigation and likely types of investigation.

The type of premises that may be inspected is another issue. This can include offices, land, vehicles and the homes of directors, managers, other employees and contractors, as well as the premises of a wholly-owned subsidiary. Linked to this is the potential need to deal with simultaneous dawn raids, involving offices and organisations in more than one EU member state or international jurisdiction.

External consequences of a dawn raid can be substantial and include reputational effects which may have long-term consequences, even if no offences are identified. It is very likely that the press will be informed about the raid and the competition authority itself may well issue a press release. Research shows that a company's share price will invariably be affected once the raid is announced, which will necessitate careful handling of relationships with shareholders and stakeholders.

It must be recognised that the internal consequences of a dawn raid are also likely to be substantial, both in the short and long term. A dawn raid is likely to involve a wide range of employees for whom this may be a challenging and demanding experience. It will also be completely unfamiliar ground to them. Preparedness, training and controlled communications are all crucial.

Overlooked aspects

It can often appear that dawn raid processes have been developed by committees of people happily ensconced in offices and operating only in business hours, with the result that the realities have sometimes simply not been fully thought through. Although not exhaustive, what follows is a starter reality checklist to ensure that the detailed practicalities have been genuinely considered:

- first-contact reception desk processes
- contact list management
- 'on the day' contact management, including deputies

- inspector's credentials and authorisations – verification
- control actions, including building management and closure
- logistics – including inspector's room allocation/ security, nominated accompanying employees, document/record copying, record-keeping of the raid and disputed document processes
- media management
- internal communications
- document preservation
- general and specific training (e.g. IT)
- dos and don'ts for employees

Dawn-raid ready

Failure to manage a dawn raid effectively can have far-reaching consequences for companies and for their employees. Moreover, failure to comply with the duty of co-operation in a dawn raid can directly result in fines being imposed, or can count as an aggravating factor when penalties are being calculated.

The overriding question, however, is how would you know if your company is genuinely ready, and prepared, in the event of a dawn raid? Internal audit offers one source of assessment, if not direct testing. Structured independent walk-throughs of a dawn raid process is another approach that has had some success. It could be argued that aggressive testing – a mock dawn raid with as near real-life situations as possible – is the only way to reveal a company's genuine, and realistic, state of readiness.

Any dawn raid will represent a significant corporate shock to any organisation, irrespective of size, location or industry. However, effective planning that considers all the likely eventualities will pay significant dividends and afford the opportunity for events on the day to be much better managed and controlled, and some of the potential consequences mitigated.

Keith Read is European knowledge leader at LRN and was formerly the group director of compliance and ethics for British Telecom (BT)

A company's share price will invariably be affected once the raid is announced