Investigating a data breach
IT Forensic Services
Overview

Within a modern commercial environment, the success of your organisation can depend upon how you use and secure information.

Data breach incidents can be high profile and damaging. They can weaken the relationship with your customers, reduce the value of your intellectual property, and attract unwanted attention from regulators and the media.

There can be a variety of motives for misappropriating company data. A desire for personal gain can drive a former employee to steal client details and intellectual property to advance their future career. Alternatively, unscrupulous individuals may seek to sell corporate data for profit or attempt to hold your organisation to ransom by threatening to leak commercial secrets to the press.

Hostile groups may seek to embarrass your company and attempt to extract data through network intrusion or by threatening and tricking your employees.

Of course, accidental loss can also occur through negligent work practices, complex organisational restructuring, or the divestment of assets.

To manage these risks companies are investing heavily in people, process, and technology to shore up their defences against attack.

Increasingly, such threats are being discussed within the boardroom as the authorities continue to hold companies and their leadership to account for the security of customer and employee data.

However, no matter how secure your defences are, breaches will occur from time to time; after all, your organisation needs to assume a degree of trust with staff. EY can help you to fully investigate and respond to these incidents when they occur.

Our IT Forensic professionals can sift through the trail that is left behind by suspects, reconstruct a timeline of events, and identify the ‘who, what, when and how’ of a breach.

We can provide advice on remedial steps to prevent recurrence and will support you throughout the lifecycle of any resulting legal action.

This brochure provides an overview of our data breach services, including the challenge faced by organisations, an approach to meeting that challenge, and some examples of previous engagements undertaken by our team.
The challenge

It is unlikely that you will know all the relevant facts once you discover a breach. Therefore, it is essential to gather as much information as possible regarding the incident and its causes so that your team can fashion an appropriate response.

All too often, organisations are thrown into panic, rash decisions are made, and evidence is lost. Many companies fail to look beneath the surface, hoping that a simple security review will fix the problem. Often this leaves the root causes of the breach undetected, fails to uncover the true extent of the breach, and subsequently exposes the company to serious risk.

A number of challenges need to be tackled head on.

Who was involved?

You need to identify all of the individuals involved in the breach. This will include not only the perpetrator and their co-conspirators, but also the victims of the breach and anyone who was ‘duped’.

Did the perpetrator work alone? Were they coerced? Did anyone ‘look the other way’?

In addition, you need to understand who in your organisation has responsibility for the compromised data sources and who is best placed to plug the leak.

The stakeholder network should be mapped as the investigation progresses. This process must be undertaken sensitively and with respect to internal social dynamics of the organisation.

How did they do it?

You will want to know the means by which the data was removed from your organisation.

Perhaps your network security was breached, or did an employee simply walk out the door with a thumb drive? Typically, a suspect will use a variety of different methods to extract data from an organisation.

You need to understand all of these methods and map the flows of the data between the source and the exit point. This will help you to understand where controls were circumvented or are absent.

What data was compromised?

This can be the most critical and difficult question to answer. What if a rogue former employee leaked customer data to the press? How do you know this was the only sensitive information that was in their possession?

You need to determine the full collection of data that the suspect has access to (directly or indirectly) over time. How much of this could have been compromised?

The suspect may have obtained the data through other individuals within the organisation – what other data sources did those individuals have access to? The output of this process will form a heat map that plots data sources according to the risk and likelihood of a breach.

When did the breach occur?

When trying to uncover the nature of a breach, investigators may focus their attention solely on the present state of the IT environment. The changes to your organisation and the events over time can be overlooked.

Over what period did the suspect have access to the data? How have controls changed over time? Has anyone else left the organisation who could have also been involved?

“… all too often, organisations are thrown into panic, rash decisions are made and evidence is lost.”
Our approach

Our data breach response teams are comprised of IT forensic and security professionals working closely with experienced corporate investigators and a background check team. We are able to work separately or as a part of your in-house incident response function. Following a breach, we will provide you with guidance on how to proceed and will always tailor our activities in accordance with your specific requirements and immediate concerns.

Securing the evidence
Initially, we will launch an incident response briefing and review the facts reported by your in-house team. We will then interview relevant staff to identify potential sources of digital evidence that need immediate forensic preservation. We can preserve a wide variety of digital evidence, covertly if required, across the globe to recognized international standards. It is vitally important that evidence is captured by a forensic professional to prevent data contamination and to strengthen legal admissibility.

Sources of evidence can include workstations, servers, database systems, mobile devices, call logs, printers, fax machines, or security systems such as CCTV and door access logs. We are experienced in the collection of complex systems, such as document management systems, complex backup tape archives, virtualised environments, or bespoke systems.

Triage
In the early phases of an investigation, it is easy to become overwhelmed with the sheer quantity of potential evidence. Our forensic triage assessment and visualisation tool can quickly identify suspicious activity for immediate analysis.

Using this approach, we can rapidly prioritise our analysis on the data sources most likely to contain evidence. For example, in addition to analysing the suspect’s work computer, we may also identify other computers that have recently accessed the compromised data source, or that have been copying and transmitting files with a similar data profile.

Investigation and analysis
We will develop an analysis strategy during the triage process. This strategy will define the tools and techniques used to uncover the facts surrounding the breach.

Our approach will be carefully phased to allow you to control, prioritise and guide the investigation.

In addition to IT Forensic analysis we can employ a number of complimentary investigative techniques. These can include investigative interviewing, data mining, and background check activities.

Reporting and expert testimony
We are experienced in presenting the results of our work to courts in Ireland and internationally. Our reports have often been used to respond to regulatory authorities, obtain search orders, and secure injunctions.

Our expert witnesses can also provide testimony in court if required.

Remediation
You may discover that the results of the investigation reveal areas of weakness in your organisation’s IT security regime.

Whilst it is impossible to adopt a security stance that completely locks down your data, our IT security professionals will be able to provide you with independent advice on data leakage prevention strategies and tools to help reduce the risk of future incidents.

“... our forensic triage assessment and visualisation tool can quickly identify suspicious activity for immediate analysis.”
Investigating a data breach

IT Forensic Services

Benefits to you

An external view
Data breach incidents are a sensitive matter and need to be managed carefully. In the early stages of an investigation, you may not be aware of who is involved, or where potentially volatile evidence may reside. As an external response team, we can provide you with an objective and unbiased method of handling the incident.

It will be important to demonstrate that your organisation is taking the matter seriously and not attempting to hide the incident from the authorities. By using an external provider, you can address these concerns by demonstrating a separation between the forensic team and the IT function.

Experienced forensic team
We only use full-time forensic practitioners for our work. We have been engaged on numerous data breach investigations and can provide you with valuable insight and experience that we have gained from numerous similar incidents.

Our IT Forensic investigators are experienced in examining digital evidence to expose the nature of a data breach. They can analyse deleted files and logs, are versed in the techniques used by hackers, and are experienced in uncovering the myriad of hidden computer artefacts that can betray the actions of a suspect, such as internet search history, removable media usage, and the use of cloud-based storage.

We can mobilise investigation teams at short notice locally or across the globe, and are able to leverage support from the global network of EY offices.

Technology
Our teams have access to a wide range of forensic capture and analysis tools. Our Advanced Solution Centers are able to provide vast amounts of processing power that enable sophisticated searches to be conducted quickly and accurately.

We have developed a number of in-house tools for data breach analysis which are continuously updated by our own development team.

Prevention, investigation and notification
Our teams can help advise you on data leakage prevention strategies and technologies, complement your investigations team and advise you on reporting and notification practicalities.

In-house training
Sometimes our clients require us to train their in-house teams on data-breach first response protocols, or to review and improve upon current policies. This training program can be customised to a specific organisation, and can incorporate mock data breach exercises.

Working with counsel
We can provide technological support to your legal counsel during any subsequent legal proceeding. We can provide expert witness testimony on the result of our analysis, and can provide litigation and e-Discovery services to assist your advisors throughout the lifecycle of a document review.

Using a triage approach to visualise data breach indicators
Our experience

Banking records
Suspect: IT Developer
Data: Customer accounts

We were engaged by a leading European Private Bank to investigate the leakage of sensitive records. The data had been stolen by a technician who had privileged knowledge of the compromised systems.

The bank became aware of the theft when a whistle-blower revealed a sample of the records that had been compromised.

Highlights
• Traced data to a variety of data sources within the bank.
• Identified emails to duped staff.
• Identified a file containing system passwords.
• Compiled a theft timeline spanning 3 years.
• Produced a report that was issued to the regulator.
• Recovered deleted computer programs that were used by the suspect to download the data.

Gas tanker contracts
Suspect: CFO
Data: Contract pricing

We were engaged by a multinational Oil and Gas client in the Middle East to investigate the leakage of commercially sensitive information. The data included details of contract pricing leaked to an industry publication.

Our client became aware of the breach when they read confidential facts within the journal that could only have been disclosed by a member of the management team.

Highlights
• Traced each item in the publication to a data source.
• Used corporate intelligence, interviews, and email analysis to identify staff with relationships to the publication.
• Analysed call and fax logs between the office and publication.

Asset divestiture
Suspect: Web Engineer
Data: Software designs

We were engaged by a retail bank to investigate the mass theft of intellectual property following an acquisition. The website engineers of the subsidiary had not destroyed designs and code that belonged to their former parent company.

The challenge for the client was being able to selectively find and destroy data that was spread across their IT landscape in an unstructured fashion.

Highlights
• Developed a forensic technique to search for proprietary design documents, source code, program binaries and testing documentation over hundreds of computers.
• Identified technical flaws in wiping software used by IT department which failed to erase data from 500 computers – despite purporting to be compliant with US Department of Defense standards.
Client data

Suspect: Sales staff
Data: Client lists

We were engaged by an insurance firm to investigate allegations that former employees had stolen proprietary product designs and were attempting to lure clients to their start-up.

The client needed to act quickly to obtain an injunction that would stop the former employees from trading with stolen material and poaching their customers.

Highlights

• Identified deleted webmail fragments containing confidential information.
• Discovered that USB devices had been used to copy client lists. Provided the serial numbers of these devices to the client.
• Helped secure an injunction against the start-up.

Database theft

Suspect: IT Developer
Data: Designs

We were engaged by an Irish manufacturing firm, whose biggest customer had cancelled their latest contract without explanation. Initial investigation revealed that the chief software developer had set-up a new company to supply software.

Highlights

• Discovered evidence of supplier collusion which helped the client secure a search order.
• Uncovered strong evidence that Intellectual Property was present on the computer systems of the developer’s new company.
• A settlement was reached based on our findings.
Contacts

Learn more
For further help and advice, please contact:

Simon Collins
+353 1 221 2176 | +353 86 838 5790
simon.collins@ie.ey.com

Julie Fenton
+353 1 221 2321 | +353 86 383 5556
julie.fenton@ie.ey.com

EY Building,
Harcourt Centre, Harcourt Street,
Dublin 2, Ireland
www.ey.com/ie/FTDS
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

© 2014 Ernst & Young, Published in Ireland. All Rights Reserved.

ED None

The Irish firm Ernst & Young is a member practice of Ernst & Young Global Limited. It is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business in the Republic of Ireland.

Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com