FORCEPOINT
POWERED BY Raytheon

Report

Europe's Insider Threats: What CISOs Need to Know

Contents

1
Executive Summary

European CISOs are locked in what appears to be a never-ending battle against cyber threats. But for many, this campaign is mainly by perceptions of external risks – attempts to breach organisations' security from the outside. There certainly are pronounced threats from cyberspace: ransomware, advanced persistent threats (APTs), targeted attacks, state-sponsored operatives and highly organised international cyber gangs.

But insider threats—from the employees within an organisation—have long been underestimated, despite being the most reputation damaging and financially destructive security risks. Worse, traditional security measures that target external attempts to access your network can't prevent insider threats nor can they defend against traditional hacking methods. Protecting the human point, where data is accessed by users and is therefore at its most vulnerable, is the key to protecting critical data.

Given that the European General Data Protection Regulation (GDPR) will come into effect in May of 2018, the clock is ticking for European organisations - they must be able to defend against insiders threats and data breaches. The GDPR will not only require organisations to notify supervising authorities and the targeted individual a breach within 72-hours, but will also levy strict penalties of up to 4% of worldwide annual turnover for serious failings. There has been little in the way of comprehensive, Europe-wide research investigating this difficult and pressing challenge in greater detail.

That is precisely why Forcepoint™ commissioned an independent survey of more than 4,000 office workers across the UK, France, Germany and Italy – to better understand attitudes toward data protection and the number of insider threats, both malicious and accidental, facing organisations within these EU member states.

Forcepoint's research[1] confirms that breaches caused by employee behaviour are the most damaging in terms of their financial and reputational impact.

2
What Are Insider Threats?

An insider threat can come from a current or former employee, a board member, or anyone has ever had access to an organisation's proprietary or confidential information.

Entities that also fall under the umbrella of an insider threat include:

- Contractors
- Business associates
- Third parties
- Individuals who have knowledge of an organisation's security practices, confidential information or access to protected networks or databases

But insider threat can take any of the following forms:

- Information theft
- Monetary theft
- Identity theft
- Data corruption or deletion
- Data altering with the intention of producing inconvenience or false criminal evidence

1 "Negligence is the Number One Cause of Insider Threats", Forcepoint Infographic, 2016 - https://www.forcepoint.com/sites/default/files/resources/files/infographic_insider_threat_negligence_number_one_cause.pdf

PwC's 2015 Information Security Breaches Survey[2] claimed that "accidental" insiders were the number one cause of breaches (26%) in the UK during the report period. In January of 2016, a mirroring Forrester report[3] came to the same conclusion. Furthermore, a Freedom of Information request sent to the Information Commissioner's Office (ICO), a data protection watchdog, revealed in June of 2016 that human error accounted for the vast majority (62%) of breach incidents over a recent three month period – far greater than the number of incidents caused by insecure web pages or hacking (9%).[4]

The headlines also reflect this trend, with major organisations suffering at the hands of malicious or negligent employees and contractors. In January 2016, UK ISP TalkTalk revealed the arrest of three call centre staff in India after charges that they had used customer details to defraud them with technical support scams[5]. In February 2016, a former employee of UK media regulator Ofcom was found to have offered his new employer – a major broadcaster – a treasure trove of sensitive data on TV companies held by the aforementioned regulator[6].

3
Key Findings

Organisations that ignore insider threats miss a critical opportunity to strengthen their security posture and provide broad protection for their companies. Key findings in this report include:

- Insider threats, both accidental and malicious, are increasing in Europe. More than one third of employees surveyed admitted their involvement in a security breach.
- There is a widespread lack of insider threat awareness. Nearly half of employees surveyed did not consider their organisation vulnerable to an insider threat.
- Data protection training and policy enforcement is inadequate across many organisations.
- The Cloud generates a great deal of uncertainty when it comes to associated security risks.

4
Where Do Insider Threats Originate?

Insider threats result from a combination of intentional and accidental employee activity, with malicious intent, staff negligence, limited security awareness and ineffective corporate policies all emerging as reasons for security breaches.

Across the UK, France, Germany and Italy, 35% of employees interviewed said they had been previously involved in a data breach.

FIG 1: Percentage of European employees involved in a data breach

5
The Awareness Gap

In part, the high level of employee involvement in data breaches can be explained by a simple lack of employee awareness.

Among survey respondents:

- 43% answered "no" when asked if their organisation is currently vulnerable to an insider threat, with a further 30% replying that they were unsure.
- Almost one third (32%) of employees said they were either unaware or unsure about breach consequences.
- Nearly one quarter (22%) of respondents said they were not aware or were not sure about the cost of data breaches to the company, and 26% said they did not know or were unclear about whether sharing work log-ins posed a security risk.

This low awareness of basic security issues is a big problem, especially since organisations rely on their staff as the first line of defence against data loss.

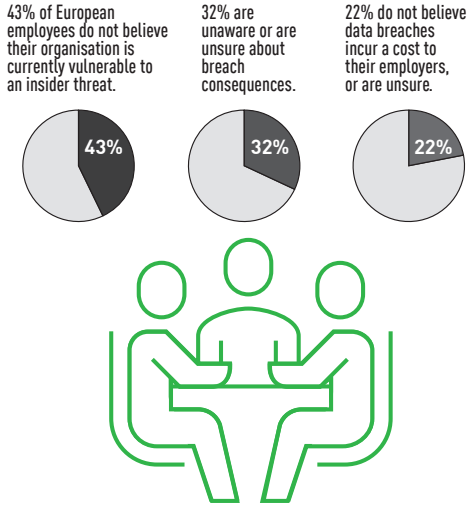


FIG 2: European employee awareness

2 2015 Information Security Breaches Survey", PwC in association with InfoSecurity Europe, commissioned by the UK Government - http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

3 "Understand The State Of Data Security And Privacy: 2015 To 2016", Forrester, January 2016 - https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2015+To+2016/-/E-RES117447

4 "Human Error to Blame as UK Data Breaches Soar", Infosecurity Magazine, June 2016 - http://www.infosecurity-magazine.com/news/human-error-to-blame-as-uk-data/

5 "TalkTalk call-centre workers arrested over customer records security breaches", Computing, January 2016 - http://www.computing.co.uk/ctg/news/2443770/talktalk-call-centre-workers-arrested-over-customer-records-security-breaches

6 "Ofcom tackles mass data breach of TV company information", The Guardian, March 2016 - https://www.theguardian.com/media/2016/mar/10/ofcom-tackles-mass-data-breach-of-tv-company-information

Cloud security also emerged as an area of great uncertainty:

- 43% of employees expressed doubt about whether their data was more or less secure in the Cloud.
- 27% of employees said that they did not consider the security of their data before uploading it to the Cloud.

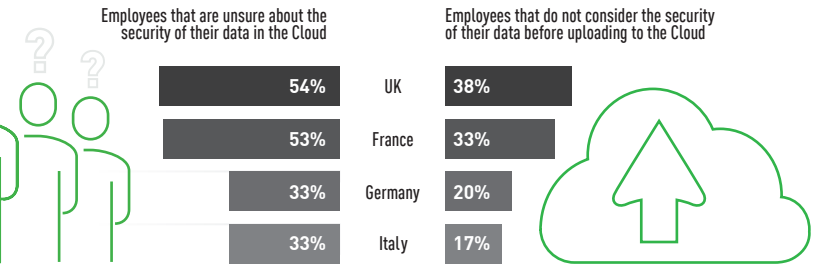


FIG 3: Awareness of data in the Cloud

Responsibility is a two-way street, and employers must ensure they give their staff a chance to understand and prevent the issues at play.

Supporting the aforementioned lack of awareness:

- 39% of respondents claimed they had never received data-protection training.
- More than one quarter (27%) of employees felt their organisations were either lacking security policies to prevent data loss or were failing to enforce them.

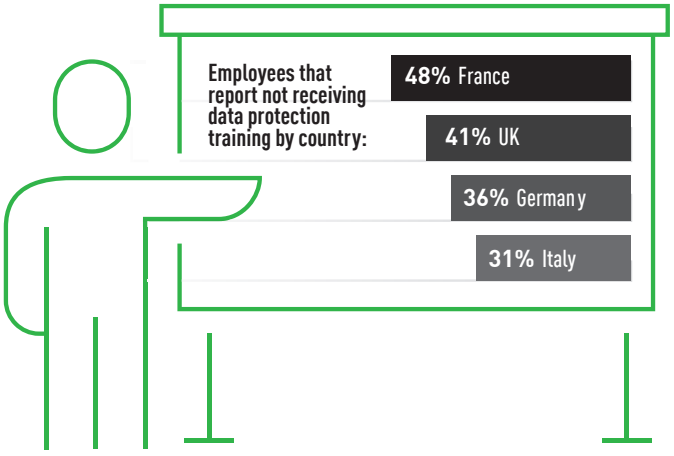


FIG 4: Data protection training and security policies

6
Accidental or Malicious?

In the course of research into organisations' security challenges, Forcepoint discovered an unacceptably high level of both accidental and deliberately risky behaviour among employees.

For example:

- 27% of respondents do not consider the security of data before uploading it. Many lose data on devices or accidentally send it out of the company.
- Across the UK, France, Germany and Italy, 17% of those surveyed claim to have lost their devices or had them stolen – rising much higher in other countries.
- 11% said they had accidentally sent information to third parties.

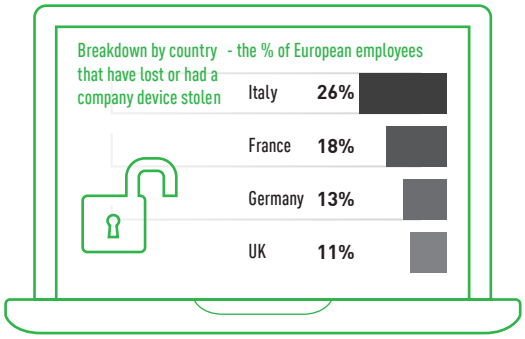


FIG 5: Overall, 17% of European employees have lost or had a company device stolen

In such cases, it is vital to have a strict policy on data use, which is rigorously enforced and supported by effective technology. But, as mentioned above, more than one quarter (27%) of staff surveyed claimed their organisation either had no policies or that they were not enforced.

Malicious intent, however, is much harder to stop:

- Some 14% of employees said they would consider selling their log-ins to a third party.
- 40% of those would do so for less than £200 – the percentage of which increases to 55% in the UK.
- Just under one third (29%) of survey respondents confirmed that they had intentionally sent unauthorised information to third parties.
- 15% of staff have taken business critical information with them from one job to another and 59% planned to use it in their next job.

There were many reasons given for these deliberate data breaches – some cited financial gain, others revenge and some even referenced moral reasons.

29 % of European employees that purposefully sent unauthorised information to a third party.

15 % of European employees that have taken business critical information with them from one job to another.
Nearly half would do so for less than £200.

14 % of European employees that would risk their job by selling their work log-ins to an outsider.
More than half of those planned to use it in their next job.

FIG 6: Malicious insider threat risks

Malicious insider activity will usually cause more damage to the organisation, as intended by the offender. Moreover, these figures reflect only those who admitted to breaking security protocols. There may be many more who would not admit to such things, even anonymously.

7
Country-by-Country Breakdown

UK

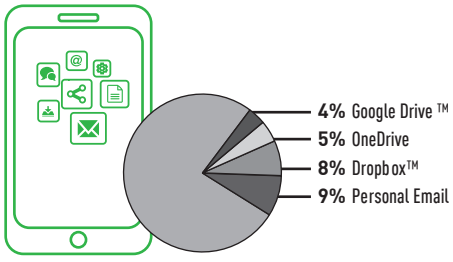
Our survey shows that more than one quarter (27%) of UK employees have suffered a breach in the past. Although this percentage is the lowest among the countries surveyed, it's still a significant number.

On the plus side, UK employees are less likely than those in the other countries to engage to engage in malicious activity. For example:

- 24% said they had purposefully sent unauthorised information to third parties – the lowest across the countries surveyed.
- 14% said they took confidential data with them when they moved jobs – the second lowest (although 68% planned to use it).

When it come to using unsanctioned cloud apps at work,UK employees are the worst offenders (9%).

FIG 7: % of UK employees that have purposefully sent unauthorised info to a third party



Despite this, awareness of security issues was particularly poor among UK respondents:

- Nearly 20% did not think their organisation was vulnerable to insider threats.
- 54% did not know if data was more or less secure in the Cloud – the highest across the UK, France, Germany and Italy.
- 38% do not consider the security of cloud apps before uploading data – which is, again, the worst in the region.

Part of this could be explained by the lack of training schemes and security policies in use among UK enterprises:

- 41% of employees claimed they had never received any training.
- 28% claimed there were either no policies in place or that policies were not enforced.
- 9% used unsanctioned cloud apps at work—among the worst of all countries surveyed.

FRANCE

In France, nearly one third of employees claim to have experienced a breach. It is the worst-performing nation amongst the countries surveyed, in terms of its lack of data protection training:

- Nearly half (47%) of respondents claimed to have never received any prior education or guidance.
- Almost half (48%) of respondents claimed they are not sure of or do not know what the consequences of a breach could be on their firm's financial health and reputation.

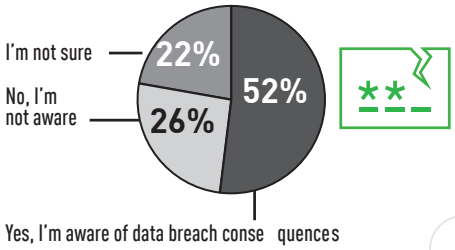


FIG 8: Are French workers aware of the consequences of a data breach?

ITALY

The survey results in Italy were alarming. An overwhelming majority of Italian employees claimed they were aware of the impact and cost of a breach on their firm's cybersecurity posture. More than half (51%) viewed sharing log-ins as a major security risk – the highest awareness rate across the region. And yet:

- Nearly half (45%) of Italian employees have been involved in a breach – the highest figure of any country surveyed.
- Italian employees were the most likely among those surveyed to have received data protection training, about 69%.
- 64% of Italian employers responded that they have widely enforced security policies in place for their companies, the highest in the region.

Awareness of security issues is not a problem for most Italians, however, this does not seem to protect employers against both accidental and deliberate data breaches.

For example:

- 12% of employees said they had accidentally sent unauthorised information to third parties – the highest number in the region.
- 30% had purposefully sent information out of the organisation to third parties – putting them at the top of the countries surveyed.
- Italian employees also had the highest number of respondents who would consider selling their log-ins (16%) and admitted to losing or having had laptops stolen (26%).

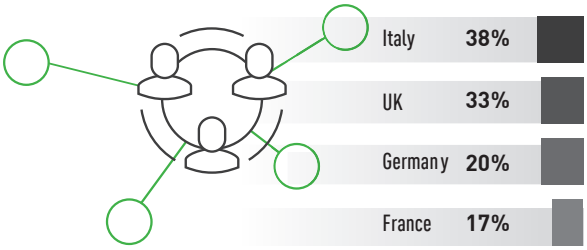


FIG 9: % of European employees that have accidentally or deliberately sent information to third parties

Perhaps the lesson from Italy is that even with strong policies and training, insider threats are difficult to mitigate.

GERMANY

Germany's employees are amongst the most aware of security issues and the least malicious insiders across the region.

- More than one third (36%) of German respondents said they had suffered a data breach.
- Even though 36% said they have never had any formal security training, 87% understood that data breaches incur a cost.
- 88% were aware that sharing log-ins is a major security risk.
- Just 33% said they were not sure how secure their data was in the Cloud, the joint lowest of the countries polled.
- 45% said they always consider security before uploading data to the Cloud.

Germans are also the second best when it comes to not using unsanctioned apps – 86% claiming they do not.

FIG 10: Data protection training and security policies

German employees do not appear willfully malicious either, with only 13% claiming to have taken data with them to their next job – among the lowest in the region. Moreover, employers appear to have a high rate of policy enforcement, 62%. The only caveat for this is that it only requires one malicious or negligent employee to create a serious insider breach. While the efforts of German staff and employers are to be praised, there is always room for improvement.

8
Research Methodology

The research was undertaken by Atomik Research, an independent creative market research agency, on a representative sample of 1000 respondents aged 18 and over in four European markets (UK, Germany, France and Italy), in accordance with Market Research Society (MRS) guidelines and regulations.

The fieldwork was completed via an online survey between July 7th and 15th, 2016. Sample sizes were as follows:

- UK – 1010 respondents
- Germany – 1012 respondents
- France – 1012 respondents
- Italy – 1021 respondents

All respondents were employed part-time or full-time and used a company or personal laptop or desktop for work.

Atomik Research is that employees MRS-certified researchers and abides by MRS code.

9
Forcepoint Solutions

To protect your organisation from a hijacked system, stolen credentials, a rogue insider or an employee's unintentional actions, you need the unrivalled visibility of Forcepoint's Insider Threat Data Protection solution.

Forcepoint Insider Threat Data Protection, for the most comprehensive insider threat solution in the industry. It does this by combining Forcepoint Insider Threat with Forcepoint DLP for the most comprehensive insider threat solution in the industry.

10
Forcepoint Data & Insider Threat Protection Security

Forcepoint is the only vendor offering an insider threat and data loss prevention (DLP) solution with visibility and behavioural analytics to baseline normal employee behaviour and quickly identify and record risky activity. These features help prevent insider theft and the exfiltration of critical data caused by malicious or accidental user behaviour.

DLP policy violations are communicated via Forcepoint's Insider Threat to easily raise awareness, monitor individual behaviour and trigger desktop video recording for attribution. All of these industry-leading capabilities are combined in one highly scalable and trusted solution that has been protecting the most sensitive organisations in the world for over 15 years.

Forcepoint's solutions complement each other. Insider Threat[7] *identifies risky users so that data protection controls can be put in place, while* Forcepoint DLP[8] identifies risky data behaviours so that users can be investigated.

FORCEPOINT INSIDER THREAT

The Visibility and Context You Need to Eliminate Insider Threats.

Forcepoint Insider Threat detects suspicious activity, whether it's a hijacked system, rogue insider or simply a user making a mistake. It ensures that your intellectual property or regulatory compliant data is not compromised.

It automatically identifies the riskiest users and provides context to unusual behaviour, including an over-the-shoulder view, enabling organisations to proactively and authoritatively address threats from within.

Forcepoint Insider Threat Key Features:

- Analytical user behaviour risk scoring engine.
- Provides early warning signs that users have been hijacked, gone rogue or are just making mistakes – before sensitive data gets breached or stolen.
- The Insider Threat Command Centre provides a highly intuitive dashboard that automatically scores and prioritises your riskiest users and quickly sees patterns that can uncover broader risks.
- Video capture and replay gives unparalleled visibility into suspicious behaviour before they become problems (e.g., creating back doors, stockpiling data, etc).
- Establishes baselines for both individual and work group behaviours.
- Searches for anomalies in an individual's behaviour to detect potential insider threats (both intentional and accidental).

Policy-Driven Identification of Risky Behaviour:

- Define specific behaviours that are known to be risky based on a set or sequence of activities.
- Detect a wide range of activity monitoring, from personally-identifiable information (PII) compliance requirements to intellectual property (IP) protection and limited malware detection.
- Fully customisable and adjustable policies weigh how user behaviour impacts the overall risk score.

7 Forcepoint's Insider Threat
https://www.forcepoint.com/product/data-insider-threat-protection/forcepoint-insider-threat

8 Forcepoint DLP
https://www.forcepoint.com/product/data-insider-threat-protection/forcepoint-dlp

Visualisation Showing Risk Score Contributors:

- An intuitive chart is generated daily for each user, allowing an investigator to quickly see what types of activities caused high risk scores.

DVR Video Capture and Replay:

- An over-the-shoulder view with screen shot captures and playback gives unparalleled visibility into suspicious behaviours before they become damaging.
- Forcepoint Insider Threat provides context and the evidence needed to attribute an incident to a user and to determine if they have been hijacked, gone rogue or are just making mistakes.
- Investigators can easily review the desktop video replay and see the user's suspicious activity at any time, allowing for attribution that is admissible in a court of law.

Timeline Activity Review and Additional Forensic Details:

- The Insider Threat Command Centre automatically scores and prioritises your riskiest users, reducing the number of daily alerts to IT teams.
- A minute-by-minute timeline quickly displays high-risk user behaviour.
- Record and playback features give visibility into the user's intent and simplifies the investigation process, intent and simplifies the investigation process.

FORCEPOINT DLP

Gain the visibility and data controls to keep critical data secure

Forcepoint DLP and Forcepoint DLP Endpoint extend data security controls to enterprise cloud applications and to your endpoints. Safely leverage powerful cloud services like Microsoft Office 365, Google for Work and Salesforce.com while protecting your sensitive data and intellectual property on Windows and Mac laptops, both on and off-network.

Forcepoint DLP Features:

- **Our unique PreciseID Fingerprinting** detects even a partial fingerprint of structured (database records) or unstructured data (documents) on Mac and Windows endpoints – whether an employee is working in the office or on the road.
- **The Industry's Only Incident Risk Ranking Dashboard:**
  - Quickly identify incidents for immediate remediation from statistical data modelling and behavioural baselining.
  - See top cluster of incidents for the previous 24 hours (midnight to midnight) and prior 7 days on the Forcepoint DLP dashboard.
  - Instantly prioritise cases from high-to-low risk levels with customisable risk score thresholds delivered in an Incident Risk Ranking report stack.
  - Know which cases exceed the risk score threshold in the designated time period that you've selected.
- **Integrated OCR** identifies sensitive data within images such as CAD designs, scanned documents, MRIs and screen shots.
- **Drip DLP** considers cumulative data transmission activity over time to identify small amounts of data leakage.
- **Behavioural-Based Policies** combine content and context awareness to automatically identify when sensitive data is being put at risk by users.
- **Data Encryption** automatically encrypts data being transferred onto removable storage devices to enable secure data sharing with partners.
- **Email-Based Incident Workflow** makes it easy to distribute an incident for review and remediation to data owners and business stakeholders without needing to provide access to the DLP management system.
- **Extend Enterprise DLP Controls** let you configure once to detect and prevent sensitive data being sent out of the organisation via email, web uploads, IM and cloud service clients.
- **Safely Deploy Microsoft Office 365** DLP Components in Microsoft to apply DLP policies in Microsoft Office 365.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[WP-EU-Insider-Threat-Survey-ENA4-200050.200317]