CLOSER THAN YOU MIGHT THINK...

The greatest risk to your data is internal – your own employees

The media is regularly awash with stories of cyber theft. Headlines abound with analysis of faceless 'hacktivist' groups such as Anonymous, or state sponsored military units in North Korea. For many businesses, such threats may seem far away and irrelevant. The harsh reality is that there are tangible risks and these are often from those you know – current and former staff and others in your supply chain.

Where are your greatest risks of data theft?

69% see those inside an organisation as the greatest threat to data security

33% of staff comfortably email data to former colleagues

22% of staff believe data theft is a victimless crime

The story of a disgruntled staff member walking off with their employer's files is one often told in management meetings. Many organisations carefully monitor staff who are about to leave and review activity after they have left the building. The sad truth however, is that it is not just 'bad leavers' that are the source of data theft.

We surveyed over a thousand white collar office workers of medium and large organisations in the UK. The findings of this research debunk myths, identifying a 'rotten core' of employees who perpetrate data theft from day one of their tenure. Whilst some of these employees claim ignorance of policies around data, many seemingly set out from their first days of employment to take their employers' confidential data.

Management should take heed of the risks from within their organisations and consider a series of initiatives around governance, communications, monitoring, and investigations to resolve the challenges identified.

THE GREATEST RISK TO YOUR DATA IS INTERNAL – YOUR OWN EMPLOYEES

> *Of the 1,100 interviewees FTI Consulting researched, 69% identified the greatest threat of data theft as being from within their own organisation.*

Perception of threat to your organisation

The greatest threat lies within

Of the 1,100 interviewees FTI Consulting researched, 69% identified the greatest threat of data theft as being from within their own organisation. Those in positions of greatest knowledge – management and compliance personnel – were even more likely to have this view – with around three quarters of these groups seeing their colleagues as the primary threat. Former staff are also noted as likely to put data at risk, with 58% of respondents identifying this group, a theme that surfaces in other areas of our research. Data leakage from these groups can be most damaging to an organisation's reputation and operations.

Whilst a large number of respondents also see external parties as presenting data security challenges, what's striking is that the groups usual touted as creating such issues are not in fact seen as such high risk. Hacktivists – anti-governmental groups are frequently cited in the media as the source of data theft, yet just over half of respondents see this threat. A higher number of compliance officers however are attuned to risks posed by this group.

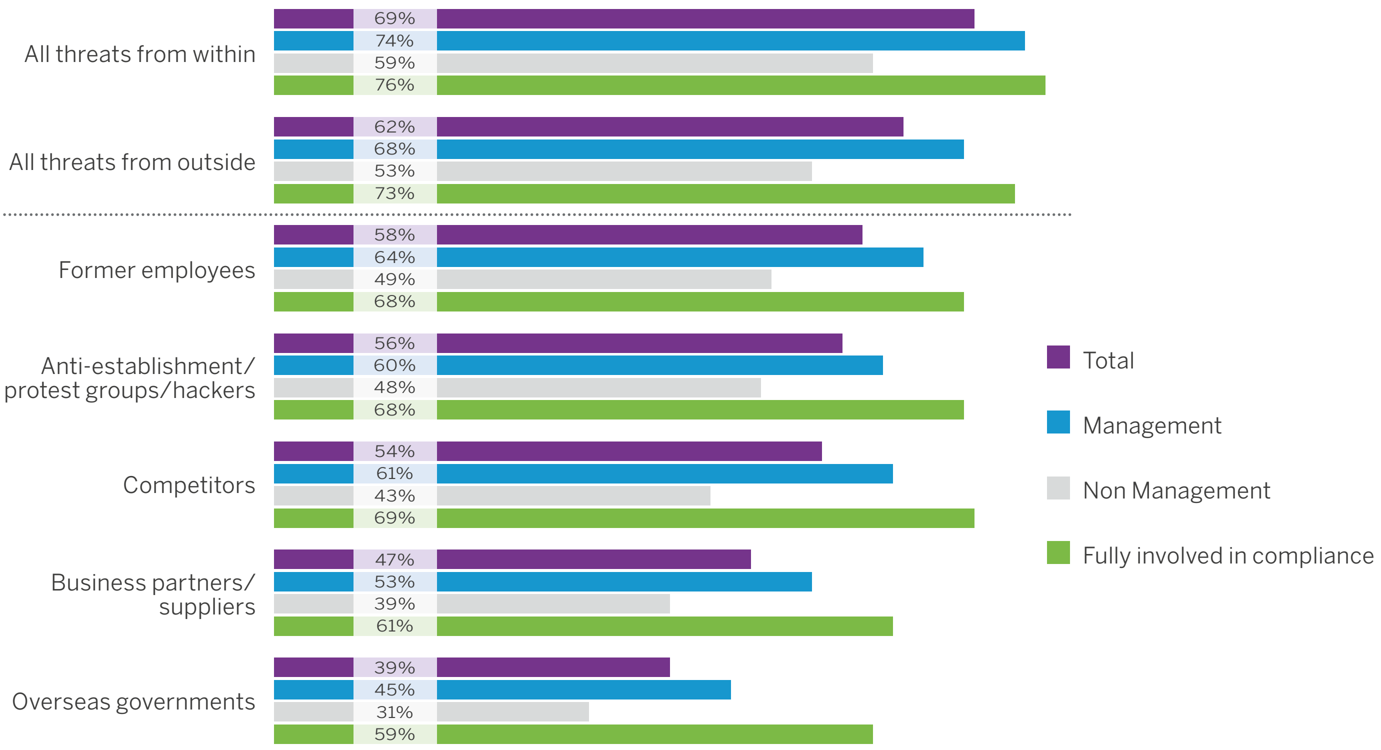
Beyond hacktivists, media coverage often identifies government backed parties as leading on industrial cyber espionage. Perhaps surprisingly, this is not borne out of the perceptions of those interviewed. Only 39% see foreign state groups as being a threat. Again a larger percentage of compliance officers cite this, but it's the lowest threat noted by those in the know.

Industrial espionage has long been seen as a major threat to corporates. Here, over half of respondents see the risk from such a source. In fact, amongst compliance personnel, this group poses the greatest external threat to data.

Perhaps surprisingly, companies should take note that those in their supply chain are a key source of risk. 47% of respondents see their business partners and suppliers as likely to put data security at risk.

Whilst the threat from outside – from competitors and others is high, management should take more notice of those within their organisations and supply chains.

Q17. To the best of your knowledge, how strong do you perceive the threat of data theft is to your organisation from the following sources?



A small but 'rotten core'

Given the surprisingly high level of threat from within an organisation, we researched employee's views on data theft, looking at attitudes and risks. Our key conclusion is that there is a small but 'rotten core' of employees who are the most likely to undertake such theft.

> *Almost a quarter (22%) of employees, consider data theft to be a victimless crime.*

Driving this threat, is the finding that almost a quarter (22%) of employees, consider data theft to be a victimless crime. This attitude suggests that tools and techniques to mitigate theft will likely always be playing catch-up unless attitudes amongst this 'rotten core' are revised, or the group is cleaned up.

Beyond the lack of concern some employees have around ownership of data, many seem unaware of any rules or policies to restrict data theft. 28% of respondents said that they did not think their workplaces had any limits on appropriation of corporate data. This suggests an internal change and communications exercise is required to inform all employees of risks and requirements.

> *22% don't require a particular event to begin thieving, instead they undertake such theft over the course of their employment.*

It may not be a surprise that some employees, whether disgruntled staff, or those shortly exiting, may take data. Our most surprising finding however is that 22% don't require a particular event to begin thieving, instead they undertake such theft over the course of their employment. This again suggests that a number of staff are predicated to data dishonesty, regardless of how they are treated or how their tenure develops.

Perhaps the most alarming finding in this area, is around the beneficiaries of data theft. Former colleagues seem to be a key destination of data sent outside an organisation – with a full third of staff personally admitting to having emailed data to former colleagues. This suggests that loyalty to former employees is higher amongst a small core, than to the employer themselves.

Management should take note of these findings. Education around risks, and communication of policies may help, but careful selection and monitoring of staff may also be required in the digital age.

Eight Key Lessons

- Carefully select both staff (full time, temporary and contract) and suppliers
- Ensure employment/supplier contracts set out that IP and other data belongs to the company
- Communicate a clear policy setting out what is allowed and what is not
- Deploy internal communications to reiterate appropriate behaviour
- Encourage whistle-blowers to come forward and raise concerns
- Plan initiatives to monitor risks and implement effective controls
- Design a response plan covering potential risks including to reputation
- Undertake a prompt and thorough investigation of any breach

METHODOLOGY

This research was conducted by FTI Consulting's Strategy Consulting & Research team in London from 21st to 23rd October 2014, involving n=1,116 white collar office workers in the United Kingdom. The margin of error is 2.9% +/- with a 95% confidence interval. Please note that the standard convention for rounding has been applied and consequently some totals do not add up to 100%.

Andrew Durant
Head of Forensic Investigations
+44 (0)20 3727 1144
andrew.durant@fticonsulting.com

Charles Palmer
Head of Reputation Management
+44 (0)20 3727 1400
charles.palmer@fticonsulting.com

Leor Franks
Marketing Director
+44 (0)20 3727 1558
leor.franks@fticonsulting.com

Dan Healy
Head of Research
+44 (0)20 3727 1239
dan.healy@fticonsulting.com

FTI™ CONSULTING

About FTI Consulting

FTI Consulting LLP. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

CRITICAL THINKING
AT THE CRITICAL TIME™

www.fticonsulting.com