quocirca

Business and IT Analysis

The trouble at your door

Targeted cyber-attacks in the UK and Europe

December 2015 – UK Edition

The research presented in this report examines the perceptions and experiences related to targeted cyber-attacks across 600 European organisations. The report includes a list of the *worst 40* reported attacks in the past 12 months. Targeted attacks are a concern for the vast majority. Almost a quarter said such attacks are now inevitable and more than one fifth admitted to a recent data theft. However, despite this bleak picture, organisations can take effective action to counter the threat.

Deployment of a range of *before*, *during* and *after* measures reduces the chances of becoming a victim in the first place and, when an incident does occur, the data losses, reputational damage and costs can be minimised. Breach response plans play a key role when the inevitable happens.

This UK edition looks at how six British organisations have ended up on the *worst 40* attacks list, including first and second place. This is despite the average British business being better prepared to defend against targeted cyber-attacks than its European counterparts.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44
Email: Rob.Bamforth@Quocirca.com

TREND MICRO

quocirca

Executive Summary

The trouble at your door

Targeted cyber-attacks in the UK and Europe

The research presented in this report has a clear message; your organisation will almost certainly be the victim of a targeted cyber-attack at some point. There is a greater than 1 in 10 chance that this will lead to serious data loss and/or reputational damage. However, putting in place certain 'before, during and after' measures can minimise the data losses, reputational damage and overall business cost of such attacks.

Targeted cyber-attacks are inevitable	Targeted cyber-attacks are considered a serious concern by nearly all European organisations; just 6% can be considered complacent, down from over 25% in 2013. In fact, 23% now consider such attacks inevitable and in the UK this figure rises to 38%. However, accepting your organisation will be targeted at some point in the future does not mean the risk cannot be reduced or that the impact of being a victim cannot be minimised.
Most organisations have already been attacked	Of the 600 organisations surveyed, 369 confirmed they had been targeted in the last 12 months (many of the remaining 231 probably had too). In 251 cases the attackers were considered to have been successful at least once. Some 133 confirmed a data theft, or were unsure if there had been a theft. 64 said it was a lot or devastating amount of data and 94 reported serious or significant reputational damage. All these figures were proportionately lower in the UK.
Many are unprepared for and lack visibility into attacks	Out of the 251 companies that acknowledged they had been successfully targeted, 31 didn't know if any data had been stolen and 6 didn't know how much. Knowing which devices, users and data have been compromised is necessary to respond effectively to a breach. However, less than half say they are able to do this and only a third currently have cyber-forensics tools in place.
The UK has been badly affected	Although overall figures in the UK were lower, six British organisations made it on to the *worst 40* list of reported attacks including the two most serious incidents, both involving costs of around €1M, devastating data loss and serious reputational damage. All six organisations already had specialist IT security teams, operations centres and/or managed security service providers in place.
Personal data is the top concern across Europe	The most commonly stolen data type is payment card or personal customer information as opposed to intellectual property. This is the top target for cybercriminals, rather than hacktivists, industrial saboteurs and nation states agents. However, as not all businesses deal with payment cards, personal customer data is the biggest overall concern, as Europeans face up to the forthcoming General Data Protection Regulation (GDPR).
All is not lost; protective measures do work	Despite the bleak picture, various *before during and after* measures to protect against or respond after targeted attacks prove to be effective. Cyber fire drills reduce impact, as does being able to detect previously unseen malware. The latter also means attacks are detected more quickly, minimising damage. A range of *after*-measures can help reduce the reputational damage and overall cost to the business of attacks.
Breach response plans are a good investment	Cost concerns drive organisations to consider breach response plans, which can reduce the cost and impact of targeted attacks. Breach response plans must go beyond clearing up and repairing damage to IT infrastructure to include proactive communication with data subjects, regulators and the media. The breach response team must extend beyond the IT department to public and media relations and senior management.

Conclusions

The threat from targeted attacks is not going to disappear, so the only practical stance is to assume your organisation will be a victim of an attack. However, it is possible to prepare for this by putting in place a range of initiatives, products and services that can have a measurable and considerable effect. Cybercrime will not go away but it can be fought.

Introduction – preparing for the inevitable

In February 2013 Quocirca published a research report (*The trouble heading for your business*[1]) looking at awareness of targeted cyber-attacks and what businesses were doing to defend against them. The research covered three major European markets: **France, Germany and the UK**.

The 2015 research published in this report takes another look at these issues, in particular asking about actual experience of targeted attacks and the effectiveness of *before, during and after measures* to defend against them. The 2015 data covers three additional markets: **Italy, the Nordic region and Spain** (see Appendix 4 for more demographic details).

There are six editions of this report, one aimed at each of the geographic markets covered in the 2015 research. This is the **UK edition**. It lists the *worst 40* attacks in Europe, six of which were in the UK, including the two most severe incidents. These attacks are those reported to have had the worst consequences in terms of reputational damage, data loss and/or financial cost to the business. The report looks at how the UK differs from the average across all regions.

Targeted attacks were clearly defined upfront for the respondents in both 2013 and 2015, as follows: "***when we refer to an 'attack' or being 'targeted' throughout this questionnaire, we are referring to a targeted attack which is an effort by an external agency to specifically penetrate your organisation's IT infrastructure using means and methods tailored for that purpose, such as custom malware and social engineering.***"

We wanted to understand the responding organisations' experience of **targeted attacks** in particular, their impact and the defences in place. So the data should not cover other security incidents such as the impact of random malware or the insider threat.

Most European organisations now accept the seriousness of targeted attacks. Almost a quarter agree they are inevitable (Figure 1). Most respondents who considered targeted attacks to be a growing concern in 2013 now accept that the problem is a long-term one that will not go away (Figure 2). In 2015 only a small number (6% across all six regions) are not concerned and can be considered complacent. This is a considerable drop since 2013 where 26% of organisations were complacent (figures for France, Germany and UK only).

Figure 1: Which of the following best describes your organisation's "view on targeted attacks"?

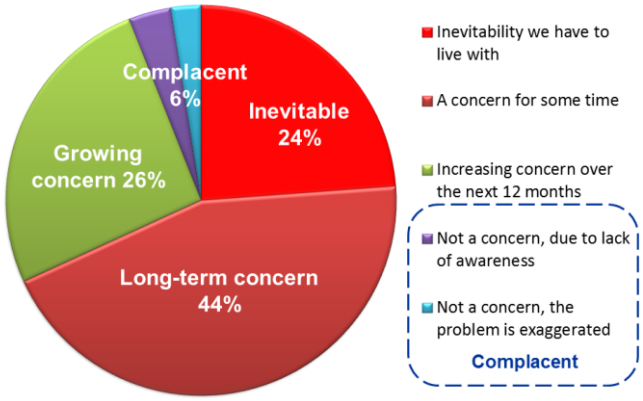
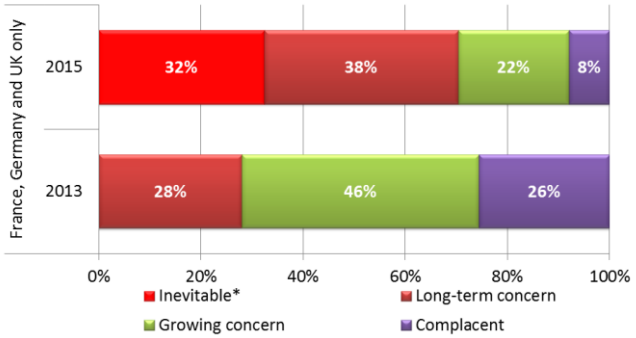
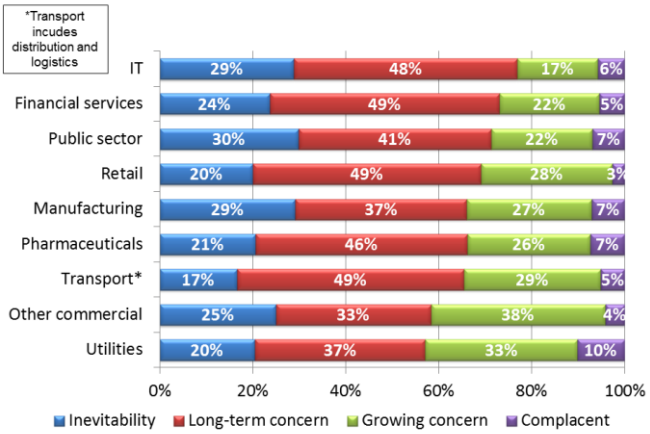


Figure 2: View on targeted attacks change from 2013 to 2015



*Note: The "*inevitable*" option was not used in 2013,

Figure 3: View on targeted attacks by sector



Across different industry sectors the IT industry tops the list, perhaps due to this sector's *insider knowledge* of the problem of cyber-threats (Figure 3). As the report will go on to show, IT is also the sector that is best prepared for the problem. Financial services, the public sector and retail are close behind; all deal extensively with personal and/or payment card data. Utilities should be more concerned as the reported data losses in this sector via targeted attacks are high. That said, no sector could be said to be highly complacent.

Being concerned about targeted attacks or even accepting their inevitability is one thing, however actually being a victim of an attack and dealing with the potential fallout is another, as reports of actual incidents will show.

The cybercrime scene

Much of the reporting from here on follows the fate over the past 12 months of the 600 organisations surveyed, aiming to understand their actual experiences. To this end, the actual numbers of samples are given in many cases as this makes the data easier to follow (percentages are used where necessary to compare between one sample and another). 369 of these 600 organisations said they had definitely been targeted (Figure 4) and all the incidents were reported as having been within the past 12 months (Figure 5). A further 95 were unsure if they had been targeted. The remaining 136 believed they had definitely not been targeted.

The report will focus mainly on the consequences of actually being targeted. But first, what of those who believe they have definitely not been attacked, or are unsure if they have been victims? Around half believe they have *effective measures to prevent* attacks (Figure 6). This really means they have not been successfully targeted rather than *definitely not been targeted*; how can you know you have escaped every sniper's bullet? The report will go on to show, that this group is indeed relatively well prepared.

The others cite various reasons for not being attacked (*been lucky, no data worth stealing, no obvious reason*). This really puts them all in the *unsure* camp. There is no good reason to believe that any organisation has *definitely not been targeted*; this is a state of mind rather than reality. However, this report is all about perceptions and if a respondent believes they have not been targeted they will also lack the information to provide further insight into actual attacks.

Figure 4: Has your organisation ever been knowingly targeted?

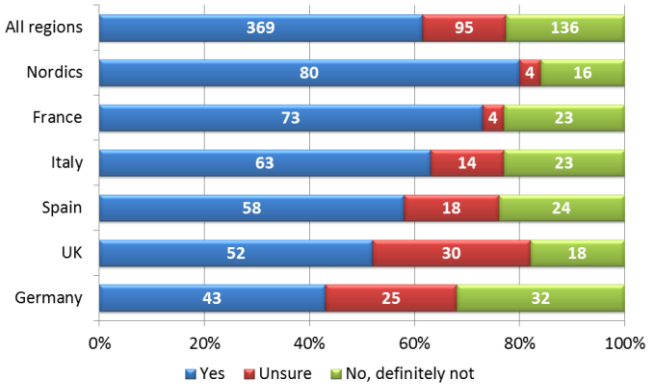


Figure 5: Timing of most recent attack for the 369 knowingly targeted

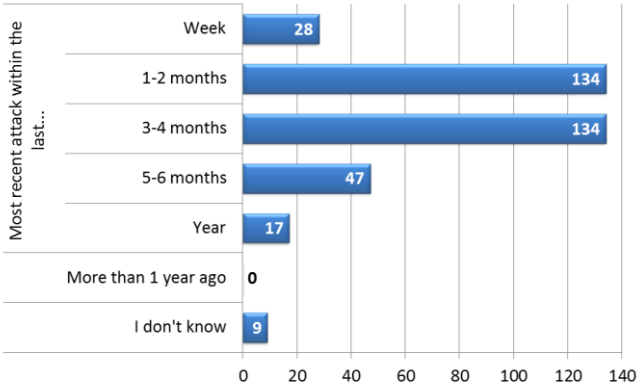
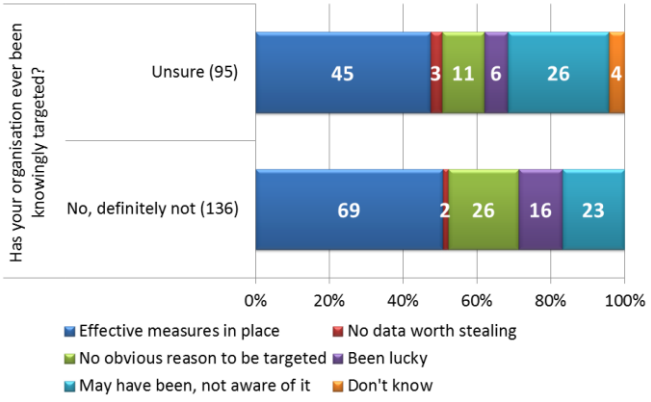


Figure 6: For those that have not been targeted, why might they have escaped (so far)?



For the 369 that admit they have been targeted the reality they perceive is stark (Figure 7). Some 251 say at least one attack has been successful; 133 had data stolen or were unsure, for 64 it was a lot or devastating amount of data and 94 reported significant or serious reputational damage. The message for any European organisation, complacent or otherwise, is that you will almost certainly be targeted, and there is a greater than 1 in 10 chance of suffering serious data loss and or/reputational damage.

Part of the reason for this is because attackers try time and again. For most that accept they have been targeted, it is more than once (Figure 8). Some 258 of the 369 (70%) said the number of attacks was increasing, while less than 5% said the number was decreasing. The more attacks there are, the more likely it is that one or more will succeed, it is then that the real damage occurs.

Figure 7: Overall European cybercrime scene and compared with the UK

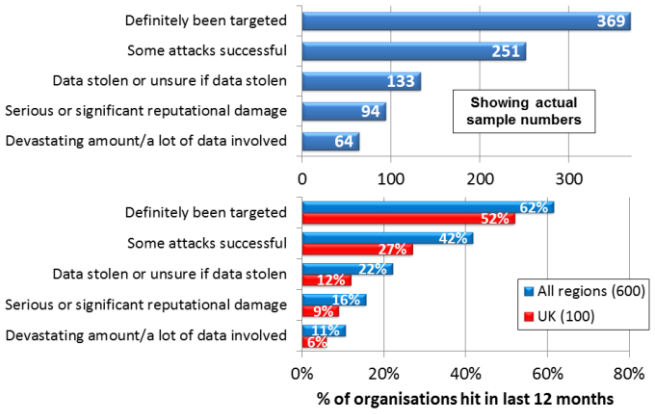
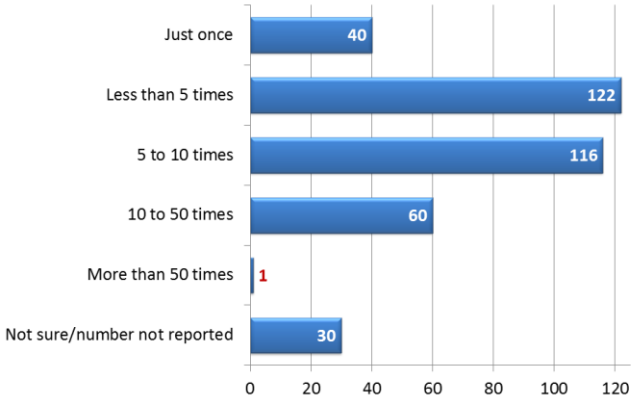


Figure 8: Estimated number of attacks in last 12 months for the 369 knowingly targeted



The damage

Of the 251 organisations that had been successfully targeted, 102 had data stolen and another 31 were unsure if data was stolen (Figure 9). For 7 it was a devastating amount, qualifying them for the *worst 40*. An attack is more likely to be reported as significant if data is stolen; however, data does not have to have been stolen for an attack to be significant. In other words, just cleaning up, even if there is no known theft of data, can be a big issue.

Figure 9: Data losses reported for 133 reporting data theft or unsure if data was stolen

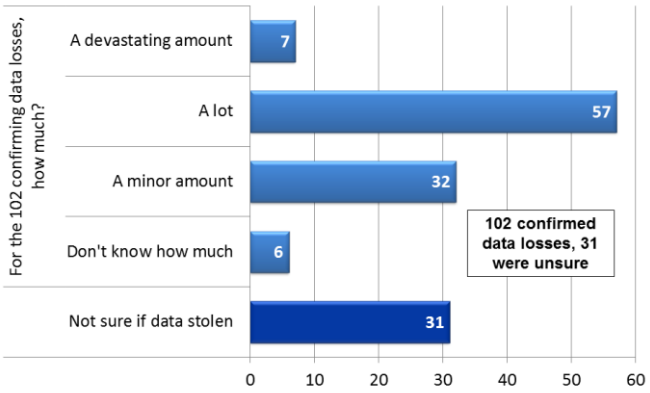
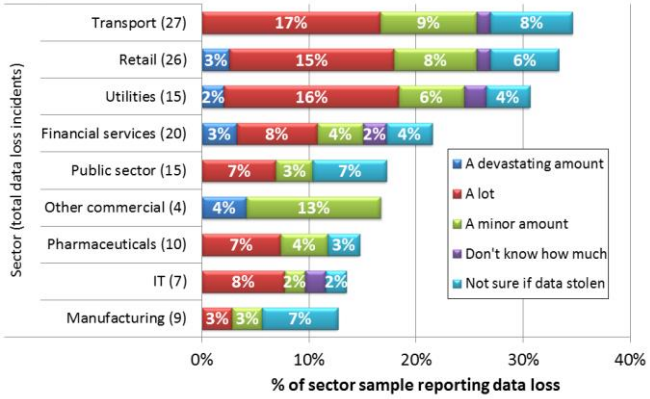


Figure 10: Data losses reported for 133 reporting data theft or unsure if data was stolen



Transport, retail and utilities top the list for the greatest proportion of organisations reporting data losses (Figure 10) in their given sector. The IT sector is one of the least impacted and there is only one IT company in the *worst 40*; as will be shown, IT is also the best prepared. The pharmaceuticals sector is the most likely to say it had *definitely not* been targeted and along with manufacturing reported some of the lowest data losses. Does dealing mainly with intellectual property make organisations less likely to be targeted and therefore more complacent? The pharmaceuticals sector appears twice in the *worst 40* and manufacturing just once.

Personal customer and payment card data were the most likely spoils, in most cases it was just one data type that was targeted (Figure 11). Attackers find what they are looking for and exfiltrate data selectively rather than downloading random data in the hope of finding something of interest later. However, one entertainment organisation (included in the commercial sector) reported an incident involving all four data types and takes the number one spot in the *worst 40*. It reported devastating data loss, serious reputational damage and an unknown high cost to the business.

Although in actual attacks payment card data is as likely to be stolen as personal customer data, across all 600 respondents the latter is of greatest concern (Figure 12). This is because many organisations do not accept online payments and those that do can take themselves out-of-scope for the main regulation, PCI DSS, by outsourcing the payment process. All organisations, however, deal with personal data to some extent and are impacted by regulations that control its privacy. They will be aware of the potentially punitive fines promised by the forthcoming EU General Data Protection Regulation (GDPR).

That said; they do not have to wait for the GDPR before the cost of targeted attacks starts to run out of control. Unsurprisingly, these costs are higher if data is stolen than if it is not (Figure 13). All those that lost a devastating amount of data reported costs in excess of €150K, as did 70% of those that lost a lot of data. Larger businesses (5,000+ employees) report higher costs of attacks, but not by much compared to smaller businesses (fewer than 5,000 employees) that will be affected worst proportionately.

Figure 11: Data types reported as stolen by the 102 confirming data losses

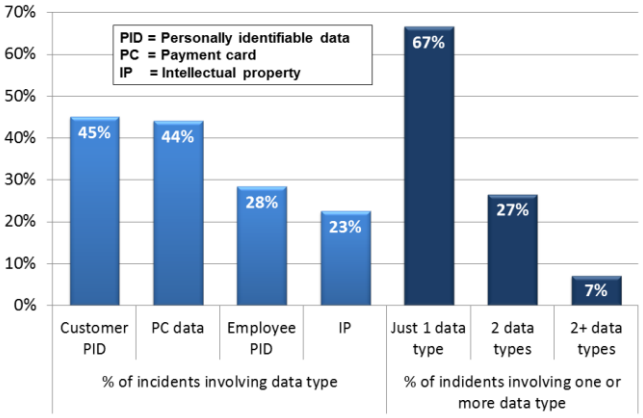


Figure 12: Data type of greatest concern, all respondents, regardless of whether they have been attacked

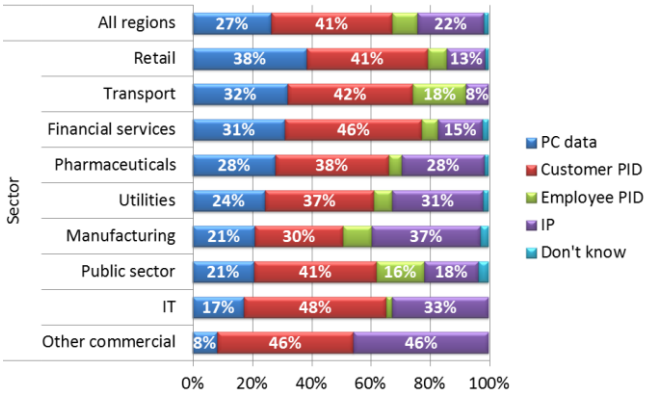
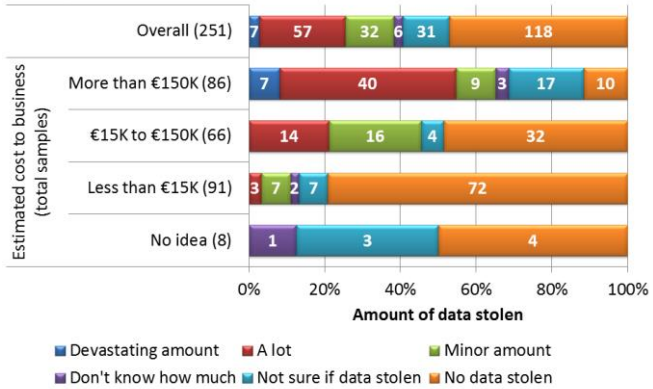


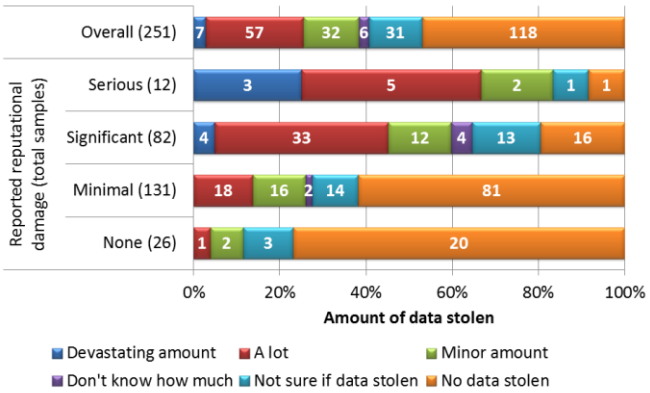
Figure 13: Cost to the business and amount of data stolen for the 251 successful attacks



None reported costs of over €1.5M. The financial impact of an attack will be a mix of clean-up costs, fines, lost business and the less tangible effect of reputational damage which increases in line with the volume of data stolen (Figure 14).

Despite being one of the sectors least likely to have suffered a data loss, IT is the most concerned about the potential impact of some future attack. The converse is true for the transport and utility sectors. Despite clear evidence about the actual damage that can result from being targeted, the message is not getting through to many about how motivated attackers are, and the range of ways in which they perpetrate their attacks.

Figure 14: Reputational damage and amount of data stolen for the 251 successful attacks



Target UK

The UK accounted for six of the *worst 40* incidents; four reporting serious reputational damage and four devastating data loss (two claiming both). All reported costs to the business ran into hundreds of thousands or millions of Euros. UK organisations took the top two places in the *worst 40*; in first place was an entertainment company and in second a utilities organisation.

UK organisations are the most likely to consider targeted attacks are now an inevitability that has to be lived with; 38% holding that view compared to 23% across Europe. UK organisations are less likely to say they have *definitely* been targeted than the European average (Figure 7), but are more likely to say *unsure* than any other (Figure 4). Is this down to more honesty or poorer visibility? Perhaps the former as the UK seems to be relatively well prepared, having the highest overall score for *before, during and after* measures (Figure 29).

In the UK, cybercriminals are of the greatest concern (Figure 15), more so than the average across all regions. The UK may be more of a focus for global cybercrime due to the widespread use of English (for example, making social engineering easier for criminals from outside the UK) and due to its large financial services sector.

The UK was the most confident about identifying and stopping attacks quickly, with 80% of those who accepted they had been targeted saying they stopped the most recent attack within five hours. The UK was the most likely to regard breach response plans as important, 89% agreeing this was so, compared to 78% in all regions (Figure 25). However, only 49% actually had a breach response plan in place compared to 42% across Europe (Figure 22).

The attackers and their methods

There are plenty of warnings from industry experts about the threat from *new* types of online attackers, especially hacktivists and nation states. However, the most worrying for most remains cybercriminals (Figure 15). This reflects the reality of reported incidents. Payment card and personal data are the prime targets of cybercriminals and the most likely data to be stolen (see Figure 11) and that 28 of the *worst 40* involved these data types, with another eight not knowing what data was stolen. In a way this is a good thing, cybercrime should be easier to defend against, as the perpetrators are unlikely to be partisan. So if your data is too hard to steal they will move on to an easier target.

In other cases, attackers will not give up. Nation state attacks and industrial espionage are more likely to target unique intellectual property (stolen in five of the *worst 40* incidents). Hacktivists usually want to disrupt or embarrass a particular organisation and will keep going until they do (two of the *worst 40* reported no data loss but serious or significant reputational damage). What is clear is the random actions of those hacking for fun are bottom of the list of concerns; this is yesterday's problem.

The attack vectors used can be grouped into two main areas; those targeted at users and those at infrastructure (Figure 16). Before investigating the level of concern about a range of vectors, Quocirca first provided the following definition: "***An attack vector is one particular means by which an attacker has tried to target your organisation. Overall a targeted attack may use a number of vectors, for example a phishing email to gain identity details followed by that identity being used to plant malware***".

Figure 15: Expected attackers: order of concern UK versus all regions

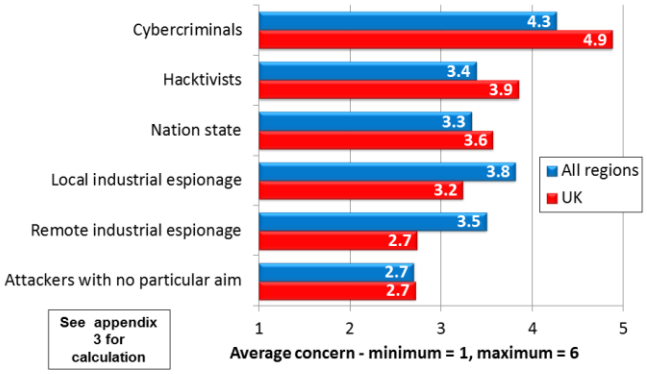
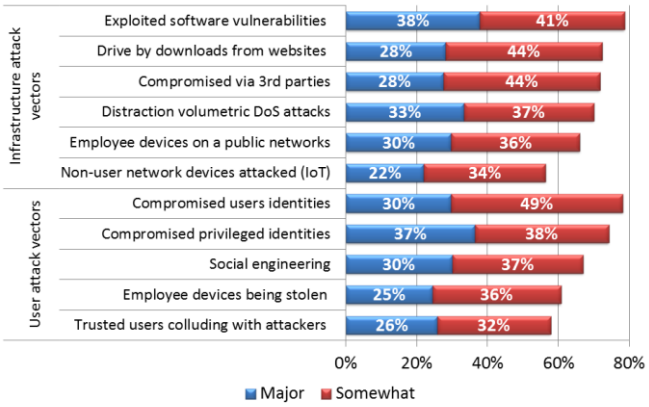


Figure 16: Concern about attack vectors



Identity compromise is considered the most worrying user-focussed attack vector; the third on the list, social engineering, is all about trying to get users to part with identity information. There is a range of user-focussed *before measures* that can help minimise such risk, the use of which is investigated in the next section.

When it comes to targeting infrastructure, software vulnerabilities and associated exploits top the list. This reflects the growing problem of systems infected with malware that is not detected by traditional signature-based methods. This may be because the vulnerability and associated exploits are previously unseen (zero day), but this is rare. More common will be malware variants with small changes that alter signatures, encrypted malware and malicious code embedded in other files (PDFs, images, documents etc.) For many it will simply be that their systems are not well enough patched to defend against known exploits or that signatures cannot be kept up to date fast enough.

Whatever the reason, the answer is to have the *during measures* in place to spot something suspicious either at the network and/or host level, and block, flag or test it. Of course, many acknowledge that some attacks will succeed and dealing with the aftermath requires effective *after measures*.

Before, during and after measures

Over 70% of organisations have a dedicated in-house security team charged with protecting against targeted attacks (Figure 17), with around 21% terming this a SOC (security operations centre). A further 11% have outsourced primary responsibility to a managed security service provider (MSSP); almost double the number in 2013. Of course, others may use an MSSP for some secondary services. 18% still entrust responsibility to the general IT team, down from over 30% in 2013.

All but five of the *worst 40* had a dedicated security function of some sort. Just having a security team is not enough to defend an organisation; it needs to be effective. Whoever is in charge, there must be a balance between putting in place a range of protective measures, making sure applications and systems remain open enough to be useful and staying within the constraints of available budgets.

Evidence that measures work helps with the decisions about where to invest. To this end, respondents were asked about their use of a range of *before, during and after measures* and then these were cross-correlated with other responses regarding the impact of targeted attacks to gauge effectiveness.

Figure 17: Prime responsibility for protecting against targeted attacks

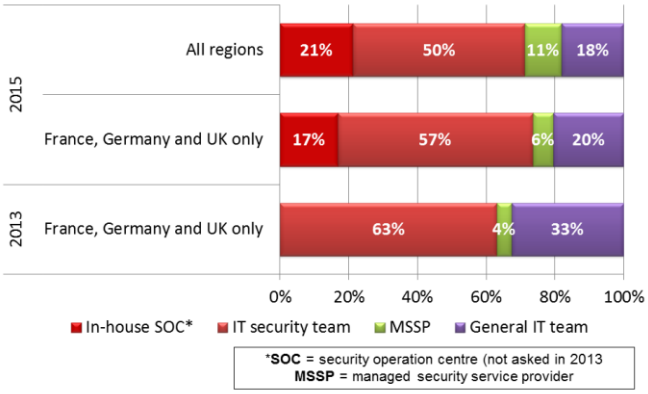
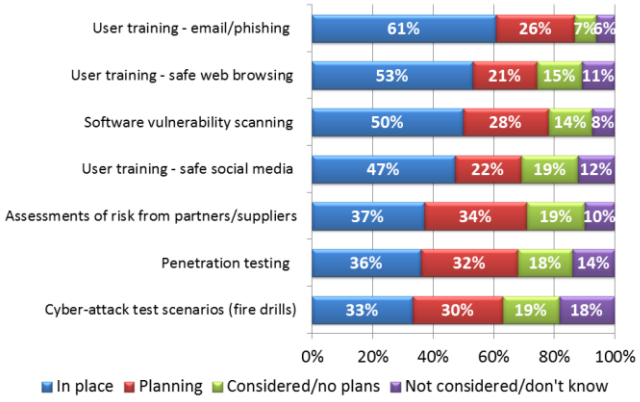


Figure 18: BEFORE MEASURES: to help prevent successful targeted attacks in the first place



Before measures

Concern about user identities being compromised leads many organisations to invest in training around safe email, web and social media use (Figure 18).

Less attention is paid to the assessment of third party risk, and more should be doing so. Exploiting weak links in supply chains has proven to be an effective attack vector, targeting small suppliers and service providers being seen as a way to hook bigger fish. Assessing third party risk reduces the impact of attacks as do cyber fire drills; those who report attacks had been stopped were twice as likely to have had cyber-attack test scenarios in place, as those that report a significant impact from attacks.

Concern about software vulnerabilities drives investment in security tools and services, especially through software vulnerability scanning and pen-testing. As a whole, *before measures* reduce the impact of attacks and improves an organisation's ability to stop them. However, they tend not to reduce concerns but are put in place as a response to rising concerns.

During measures

Detecting targeted email attacks such as spear-phishing is the most widely deployed *during* measure (Figure 19). Breach detection technology and network traffic analysis are also high on the list. These are effective ways of detecting the exfiltration of data and for many will have been deployed for some time, as much to counter the insider threat as targeted attacks.

With the right capabilities, network traffic can also be monitored for incoming threats, this may include the use of sandboxes. Should malware escape detection and end up on user devices and/or servers, then application white/black listing can make sure it does not actually run.

Some 47% of respondents have deployed some sort of technology, which they believe can *detect previously unseen malware*. Deployment is higher among those who stop or limit the impact of targeted attacks than for those who suffer a significant impact (Figure 20). For those who say they have *definitely not* or are *unsure* if they have been targeted, deployment also varies. Those that claim they were saved by effective measures are more likely to have such technology in place. Apart from a lucky few, the others were some of the least likely to do so (you can be prepared and lucky!)

For those that have been targeted, the reported time to *identify* and *stop* attacks varies from hours to weeks. Of course, in many cases it will not be that clear when the elements that constitute a targeted attack were first put in place. Other data sources suggest average residency time for targeted malware running into weeks and months. Nevertheless, those with either sandboxes or technology to *detect previously unseen malware* are more likely to report fast detection and hence limit impact (Figure 21).

Figure 19: DURING MEASURES: to help detect and stop attacks in progress

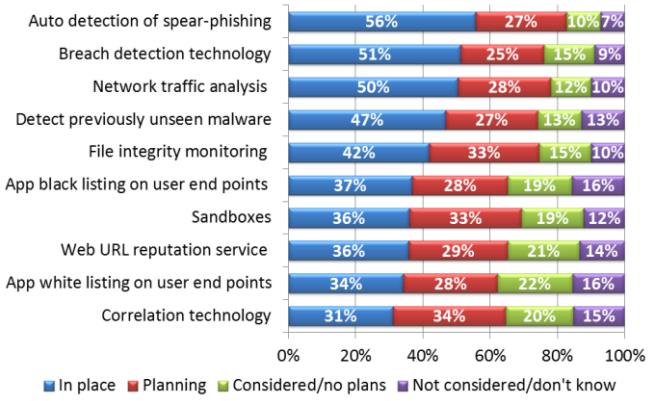


Figure 20: DURING MEASURES: technology to detect previously unseen malware by attack status

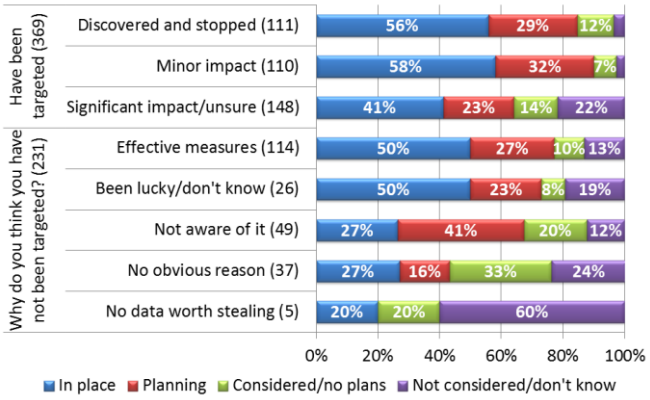
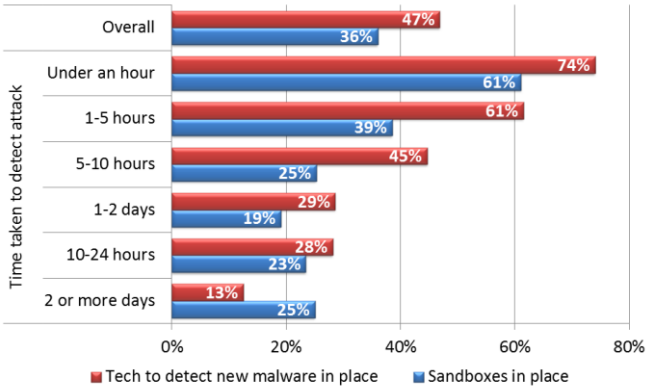


Figure 21: DURING MEASURES: time to stop attack and use of sandboxes and malware detection



After measures

The majority of organisations have basic tools in place for cleaning up malware (Figure 22), but that may be the least of their problems if data has been stolen. Knowing which devices, users and data have been compromised is necessary for an effective response after a security incident. However less than half say they are able to do this and only a third currently have cyber-forensics tools in place.

More after measures in place means less reputational damage (Figure 23), with the exception of the small number (12) that reported *serious* reputational damage, with big data losses and high consequent costs (see the *worst 40* in Appendix 1). They may of course have been moved to improve *after measures* significantly after the attack that led to this, or it may just reflect the fact that ultimately all organisations are vulnerable to targeted attacks. None of the 12 organisations that suffered serious reputational damage were complacent in their view of targeted attacks.

The different tasks that need to be undertaken following an incident can be pulled together in a **breach response plan**, which 42% of respondents said they currently had. The ability to clean up malware and identify compromised data, users and systems, are just the backroom elements of such plans, as the next section will discuss.

More should put such plans in place; those reporting minimal or no impact from a successful targeted attack were twice as likely to have a breach response plan than those who reported significant or serious damage (Figure 24). Even planning to put one in place seems to make a difference, because organisations going through that process will already be more aware of what is needed.

Figure 22: AFTER MEASURES: to help clear up after successful attacks

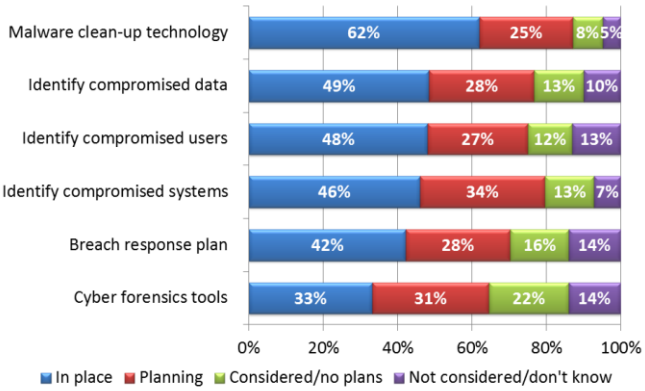


Figure 23: AFTER MEASURES and reputational impact of actual attacks (see Appendix 3)

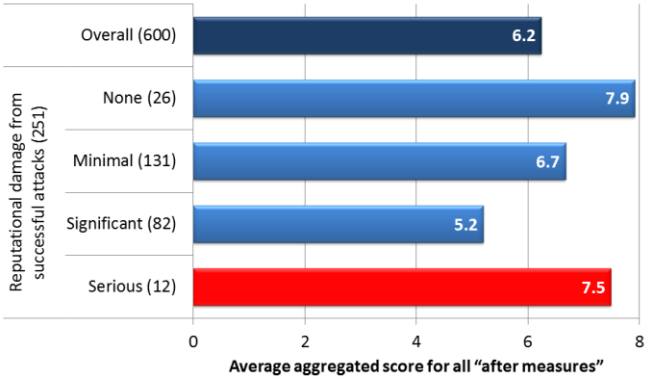
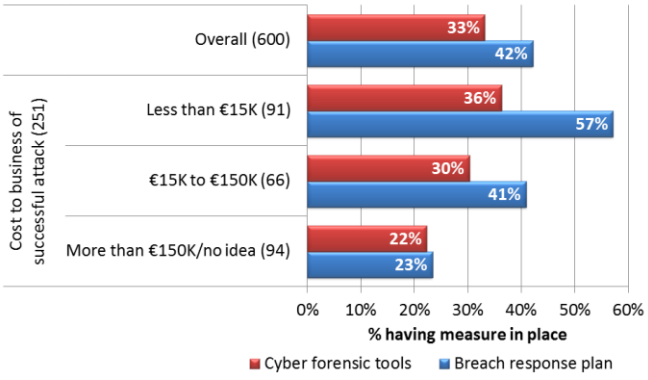


Figure 24: AFTER MEASURES and cost of actual attacks



Breach response plans

It may be that only 42% have breach response plans in place, but almost 80% recognise their importance (Figure 25). Only 6% say they are unimportant. The IT sector tops the list, again setting an example.

As demonstrated in the last section, having a plan in place reduces the reported costs of actual attacks; i.e. breach response plans work. However, correlated data across all respondents shows that the higher the acknowledged cost of a potential targeted attack, the more likely an organisation is to consider a breach response plan. And when thoughts turn to action, experience of actual attacks shows that putting plans in place is worth the effort.

The best breach response plans work because they are about more than clearing up the mess within a breached organisation's IT infrastructure. They are also about managing external entities that are impacted by, or have an interest in, the breach. To this end, the need to have a process for informing data subjects is recognised as important by 74% (Figure 26) and doing this as effectively as possible will include media management, recognised as important by 64%. A similar number believe plans should include how to liaise with regulators. In reality, those that do not recognise the need for such external communications must either deal with little or no personal data or have the misguided view that data breaches remain purely an issue for the IT department.

Effective communication means building a breach response team that extends well beyond IT (Figure 27). All such teams included individuals from the IT security team and/or the general IT team to provide background information on what has happened. Those that have experienced *serious* reputational damage are more than twice as likely to say media management is important.

Figure 25: Importance of pre-defined breach response plans

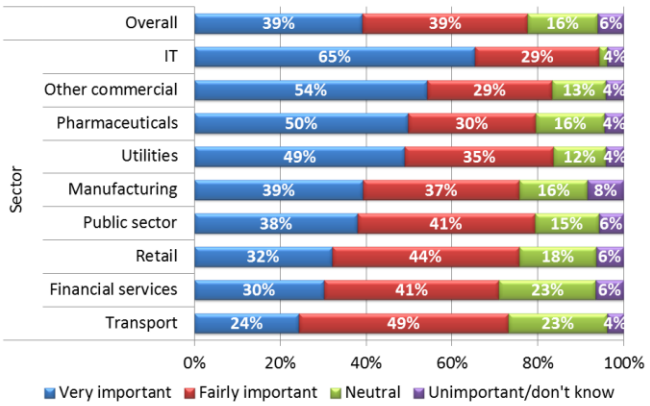


Figure 26: Importance of elements of a breach response plan

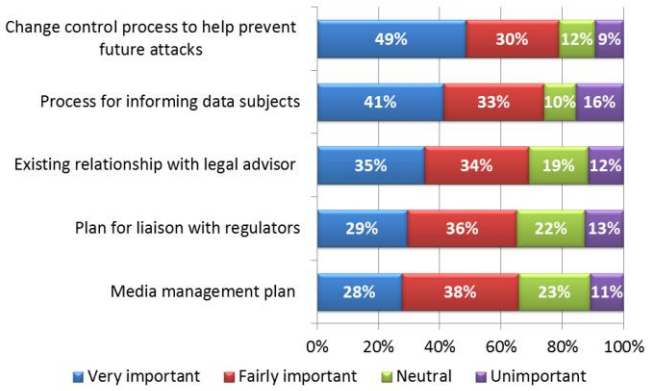
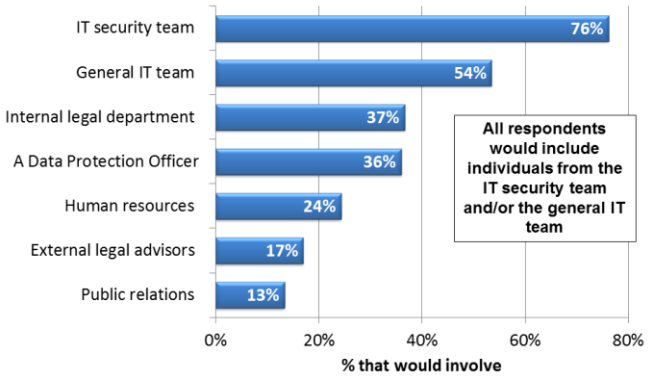
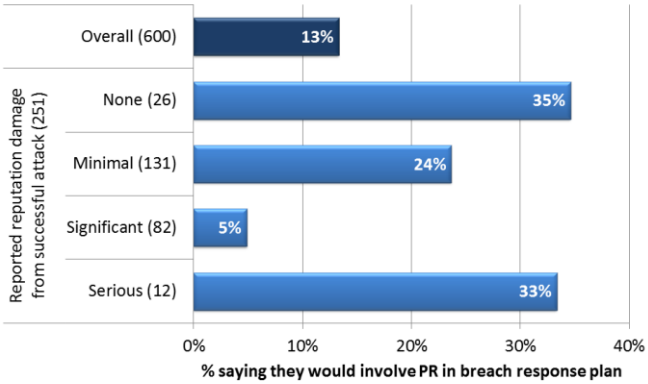


Figure 27: Departments and roles that should be involved in a breach response team



When it comes to the crunch, having PR involved in breach response plans does seem to work (Figure 28). Except in the most extreme circumstances, those reporting no or minimal reputational damage were more likely to have involved PR than those reporting significant damage. The 12 reporting serious reputational damage were also likely to turn to PR. This may be a view they have developed after the event.

Figure 28: Reputational damage and involvement of public relations (PR) in breach response plans

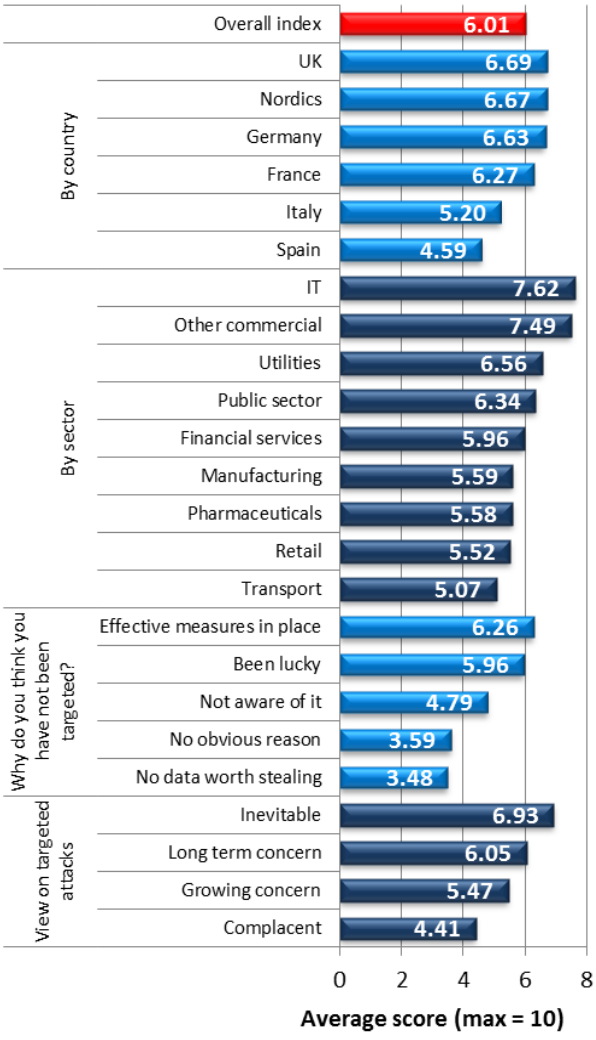


Conclusions

The 600 organisations interviewed for this report have confirmed the sheer scale of targeted cyber-attacks in Europe. The incidents listed in the *worst 40* have had a major impact on those organisations involved and these are just the most serious cases – there are many others. The majority involved the theft of payment card and/or personal data – the favoured target of cybercriminals, who are the attackers of greatest concern to respondents

However, there is good news. Cybercriminals are easier to defend against, in that they will move on to another organisation with weaker defences if yours are too strong. There is plenty of scope for getting ahead, a score can be calculated for the *before, during and after measures* an organisation has in place (Figure 29). The overall average for our 600 respondents is 6.01/10. Some countries, including the UK, do better than average, as do some industry sectors, with the IT sector setting an example at the top of the list. However, all could do better.

Figure 29: Overall scores for deployment of before, during and after measures (see Appendix 3)



This report started by looking at the concerns organisations have about targeted attacks. The greater the level of concern, the more likely they are to have invested in measures to prevent, manage and cope with the aftermath of attacks (Figure 29, bottom). However, the fact remains, that there are organisations which know they have been targeted, but do not know if they have lost data as a result or how much. It is clear that greater visibility is needed into breaches in order to respond effectively

As for those that believe they have not been attacked they are almost certainly misguided. Those that felt this was because they had *effective measures* in place are justified in saying so, but those that felt there was no reason they would be attacked had few defences in place and in reality have no idea if they have been attacked or not. Concerns about targeted attacks are well placed and investment to minimise their impact has a measurable and considerable effect. Cybercrime will not go away but it can be fought.

Appendix 1: The *worst 40* reported incidents

The *worst 40* incidents are those reported as having serious reputational damage (12), involving devastating data loss (7) or incurring costs to the business in excess of €750K (25). There is overlap between the three groups leaving a total of 40.

IP = intellectual property
PI = personal customer data
ED = personal employee data
PC = payment card data
NS = not sure if data stolen
DK = don't know
NSR = No specific responsibility

Rank	Country	Sector	Business size	Reputational impact	Amount of data stolen	Data types	Estimated cost to business	Security setup
1	UK	Entertainment	Mid-market	Serious	Devastating	All	No idea – a lot	IT security team
2	UK	Utilities	Enterprise	Serious	Devastating	PI	€750K-€1.5M	MSSP
3	Spain	Finance	Mid-market	Significant	Don't know	PC	€750K-€1.5M	IT security team
4	Italy	Finance	Enterprise	Significant	A lot	IP	€750K-€1.5M	In-house SOC
5	Italy	Transport	Enterprise	Significant	A lot	PC	€750K-€1.5M	In-house SOC
6	Spain	Finance	Mid-market	Significant	A lot	PI	€750K-€1.5M	NSR
7	Spain	Retail	Enterprise	Significant	A lot	PI	€750K-€1.5M	In-house SOC
8	Spain	Retail	Enterprise	Significant	A lot	PC	€750K-€1.5M	MSSP
9	Spain	Utilities	Enterprise	Significant	A lot	PI	€750K-€1.5M	MSSP
10	Germany	Finance	Mid-market	Significant	NS	DK	€750K-€1.5M	General IT team
11	Italy	Finance	Enterprise	Significant	NS	DK	€750K-€1.5M	Not sure
12	Italy	Retail	Mid-market	Significant	NS	DK	€750K-€1.5M	In-house SOC
13	Italy	Finance	Enterprise	Significant	NS	DK	€750K-€1.5M	In-house SOC
14	Italy	Transport	Mid-market	Significant	NS	DK	€750K-€1.5M	MSSP
15	Spain	Finance	Enterprise	Significant	NS	DK	€750K-€1.5M	IT security team
16	Italy	Finance	Enterprise	Minimal	A lot	DE	€750K-€1.5M	IT security team
17	Italy	Manufacturing	Enterprise	Minimal	A lot	PI	€750K-€1.5M	IT security team
18	Italy	Transport	Enterprise	Minimal	A lot	PI	€750K-€1.5M	IT security team
19	Italy	Transport	Enterprise	Minimal	A lot	PC	€750K-€1.5M	In-house SOC
20	Italy	Retail	Enterprise	Minimal	A lot	PC	€750K-€1.5M	MSSP
21	Spain	Retail	Enterprise	Minimal	A lot	PC	€750K-€1.5M	In-house SOC
22	Spain	Transport	Enterprise	Minimal	A lot	PC	€750K-€1.5M	In-house SOC
23	Spain	Retail	Mid-market	Minimal	A lot	PC	€750K-€1.5M	MSSP
24	Spain	Retail	Enterprise	Minimal	NS	DK	€750K-€1.5M	IT security team
25	Italy	Services	Not know	Significant	Minor	IP/PC	€750K-€1.5M	In-house SOC
26	Italy	IT	Enterprise	Significant	None	None	€750K-€1.5M	IT security team
27	Italy	Finance	Mid-market	Significant	Devastating	PI	€400k-€750K	MSSP
28	UK	Finance	Mid-market	Significant	Devastating	PC	€400k-€750K	In-house SOC
29	UK	Retail	Mid-market	Significant	Devastating	PC/PI	€400k-€750K	In-house SOC
30	Germany	Finance	Enterprise	Serious	A lot	PC/PI	€400k-€750K	IT security team
31	France	Finance	Enterprise	Serious	Devastating	PI	€150K-€400Kk	In-house SOC
32	France	Retail	Enterprise	Significant	Devastating	IP/PC	€150K-€400Kk	General IT team
33	Denmark	Pharmaceuticals	Enterprise	Serious	A lot	IP	€150K-€400Kk	General IT team
34	Norway	Retail	Mid-market	Serious	A lot	PC	€150K-€400Kk	MSSP
35	Norway	Retail	Mid-market	Serious	A lot	PC/PI	€150K-€400Kk	MSSP
36	UK	Retail	Enterprise	Serious	Minor	PC/PI	€150K-€400Kk	IT security team
37	Finland	Pharmaceuticals	Mid-market	Serious	A lot	PI	€75K-€150K	In-house SOC
38	UK	Utilities	Enterprise	Serious	NS	DK	€75K-€150K	In-house SOC
39	France	Finance	Mid-market	Serious	Minor	PC/PI	€15K-€75K	IT security team
40	France	Public sector	Mid-market	Serious	None	None	€1.5K-€15K	In-house SOC

Appendix 2: References

1: The trouble heading for your business, Quocirca, February 2013
http://quocirca.com/content/trouble-heading-your-business

Appendix 3: Calculations

Actors – Figure 15

Respondents were asked to place the six actors in order. The one at the top of their list was scored 6 and the one at the bottom was scored 1. An average score could then be calculated for the concern about any given actor. If all 600 had selected the same actor as their top concern it would have scored 6, if all have selected the same one as their bottom concern it would have scored 1.

Scoring before, during and after measures – Figure 23 and 29

An overall score can be calculated for each *before, during and after measure*:

Score of 10 for *in place*
Score of 5 for *planning*
Score of 1 for *considered/no plans*
Score of 0 for *never considered*
Score of 0 for *don't know*

These scores can then be averaged to provide an overall score for *after measures* as has been used in Figure 23 or for all *before, during and after measures*, as has been done in Figure 29. If an organisation had all measures in place it would score 10, if it had none in place it would score 0.

Appendix 4 demographics

All respondents were senior IT decision makers who confirmed they had an understanding of their organisation's IT security capabilities. Figure 30 and 31 show the break down by country, sector and size.

Figure 30: Countries and industries

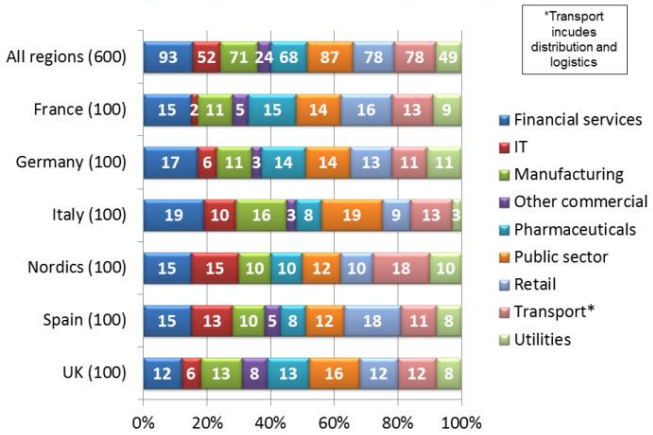
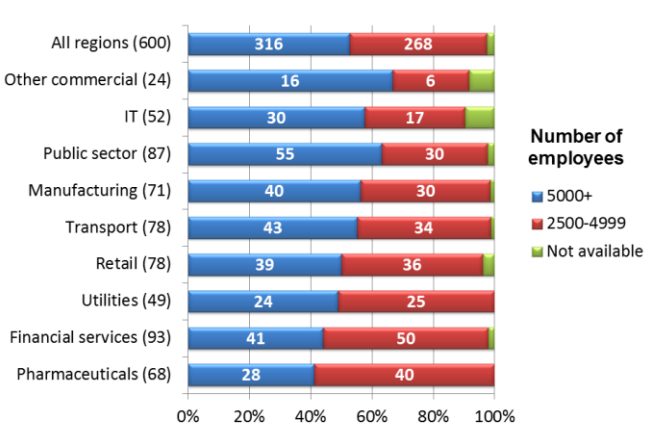


Figure 31: Industries and organisation size



About Trend Micro

As a global leader in IT security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With over 25 years of security expertise, we're recognized as the market leader in server security, cloud security, and small business content security.

Trend Micro security fits the needs of our customers and partners. Our solutions protect end users on any device, optimize security for the modern data center, and secure networks against breaches from targeted attacks. We deliver top-ranked client-server, network, and cloud-based protection that stops new threats faster, detects breaches better, and protects data in physical, virtual, and cloud environments.

Our security is powered by Trend Micro™ *Smart Protection Network*™ global threat intelligence and is supported by over 1,200 security experts around the world.

For more information, visit www.trendmicro.co.uk. Or follow us on Twitter at @TrendMicroUK.

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With worldwide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long-term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

quocirca