KPMG
cutting through complexity

Risk Consulting

An ethical investigation into
cyber security across the Forbes 2000

Publish and be Damned

What does your online
corporate profile reveal?

Cyber Vulnerability Index 2012

Foreword

Following a series of very high-profile security breaches over the past year, executives are quickly becoming aware of the significant risks posed by the loss of data: competitive advantage is eroded; organisational secrets are stolen; corporate reputations are damaged.

Today's cyber attack threat has evolved significantly from the rather crude 'full frontal attack' method that characterised attacks in the past. Indeed, today's cyber threat is more likely to come from social activists, criminals, competitors or even national governments who use stealth tactics to identify and exploit publicly available information with the ultimate goal of gaining unfettered access to networks and systems.

Modern cyber attacks prey on "information leaks" - publicly accessible information relating to organisations and their employees which is then used in targeted phishing or "spear-phishing", elaborate social engineering and technical attacks against entire organisations.

Due to the public nature of information leaks, which are often inadvertent, this phase of cyber attacker reconnaissance typically leaves little or no footprint, yet can allow for gathering of confidential internal usernames, email addresses, network details and vulnerable software versions to list but a few examples.

Here is how it works: let's say, for example, that you made a donation to a local charity, in recognition the organisation lists your name on their website as a sponsor. Two days later, you receive an email from the Fundraising Chair asking you to confirm your donation. You open the email, fill out the form (being careful not to include any banking or sensitive information) and return it to the sender. But in reality, the email didn't come from the charity at all; the attachment was, in fact, a high-quality fake containing a virus, allowing perpetrators to seize control of your computer, read your emails and record your passwords. Everything you know, they now know; everything you see, they now see. Clearly, information leakage is rapidly becoming a board-level risk. But exactly how big a risk is it?

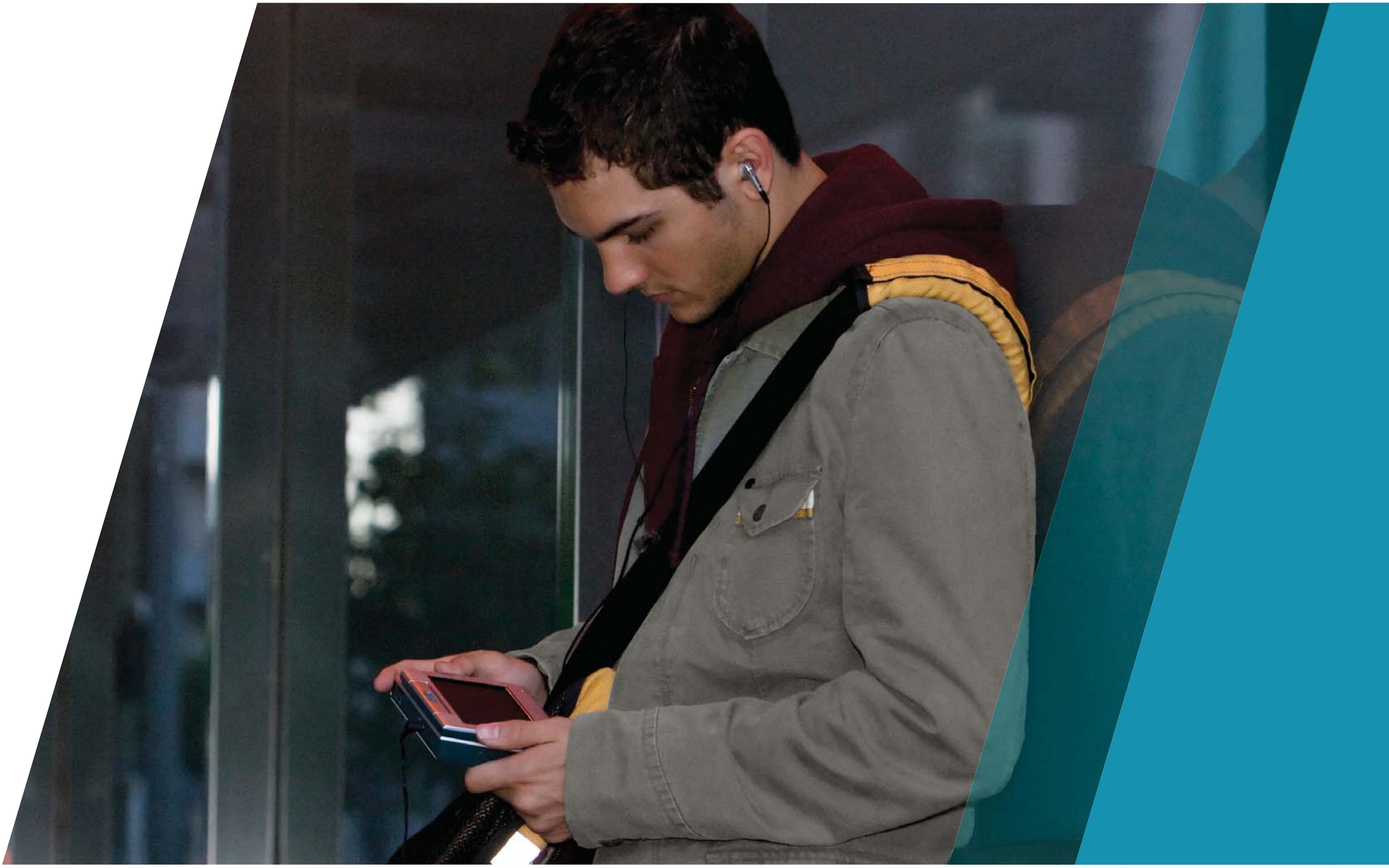
Over a six month period KPMG performed research in this domain focussing on the Forbes 2000: an annual ranking of the top 2000 public companies in the world by Forbes magazine. At the inception of this research the combined market value of all Forbes 2000 companies was US$31 trillion. The aim of this research was to perform the same initial steps that cyber attackers and organised criminals would perform when profiling a target organisation for attack, using sophisticated techniques that are often referred to as Advanced Persistent Threats, or 'APTs'.

By performing the same study across the Forbes 2000 it was possible to identify common themes and trends across countries and sectors. The research identified many security shortfalls in the Internet-facing security posture of organisations and specific countries. No hacking, unauthorised or illegal actions were performed during this research. The information leaks gathered were sourced from publically available information, search engines, and public documents located across the Forbes 2000 corporate websites. The results provide an insight into missing security basics which are exposing websites, employees and corporate data to potential cyber attack.

This report provides an overview of our findings and paints a picture of a world that has yet to come to terms with the threats posed by cyber attackers. As such, these results should provide executives with not only a strong incentive for greater awareness and management of their organisation's information, but also provide a unique benchmark against which to measure their security activities.

I encourage you to contact either myself or your local KPMG office to learn more about these findings or to discuss your organisation's exposure to these critical risks.

Martin Jordan
Head of Cyber Response
KPMG in the UK



Contents

Executive Summary

With so many cyber attacks in the news recently, executives are becoming increasingly concerned about their organisation's exposure to hackers. And so they should. According to our research, more than three-quarters of the Forbes 2000 companies leak potentially dangerous data.

The sources of this information are varied and widespread. Some are within the direct control of the corporation (websites, documents and web servers) and – with effort – can be directly addressed. Other channels such as popular search engines and forums, are outside of the usual enterprise security curtain and pose a much more complex challenge.

Interestingly, many of the sectors that normally display exceptionally strong cyber security controls seem to be at the highest risk, namely banks, financial services and telecoms companies.

The problem is also not unique to one region or market type in particular. Indeed, looking at the 'Heat Map' of global information leakage across the Forbes 2000, higher-risk countries span both the developed world (US, Switzerland, Japan, and Germany to name a few) and the emerging markets (such as Brazil, Thailand and Saudi Arabia).

Figure 1

Top 10 information leaking sectors

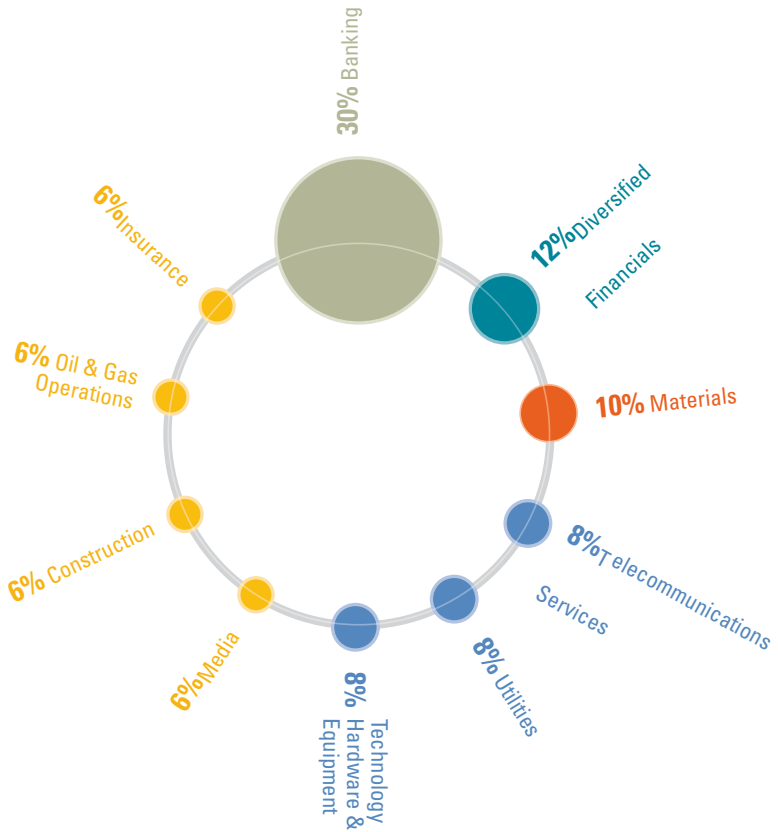
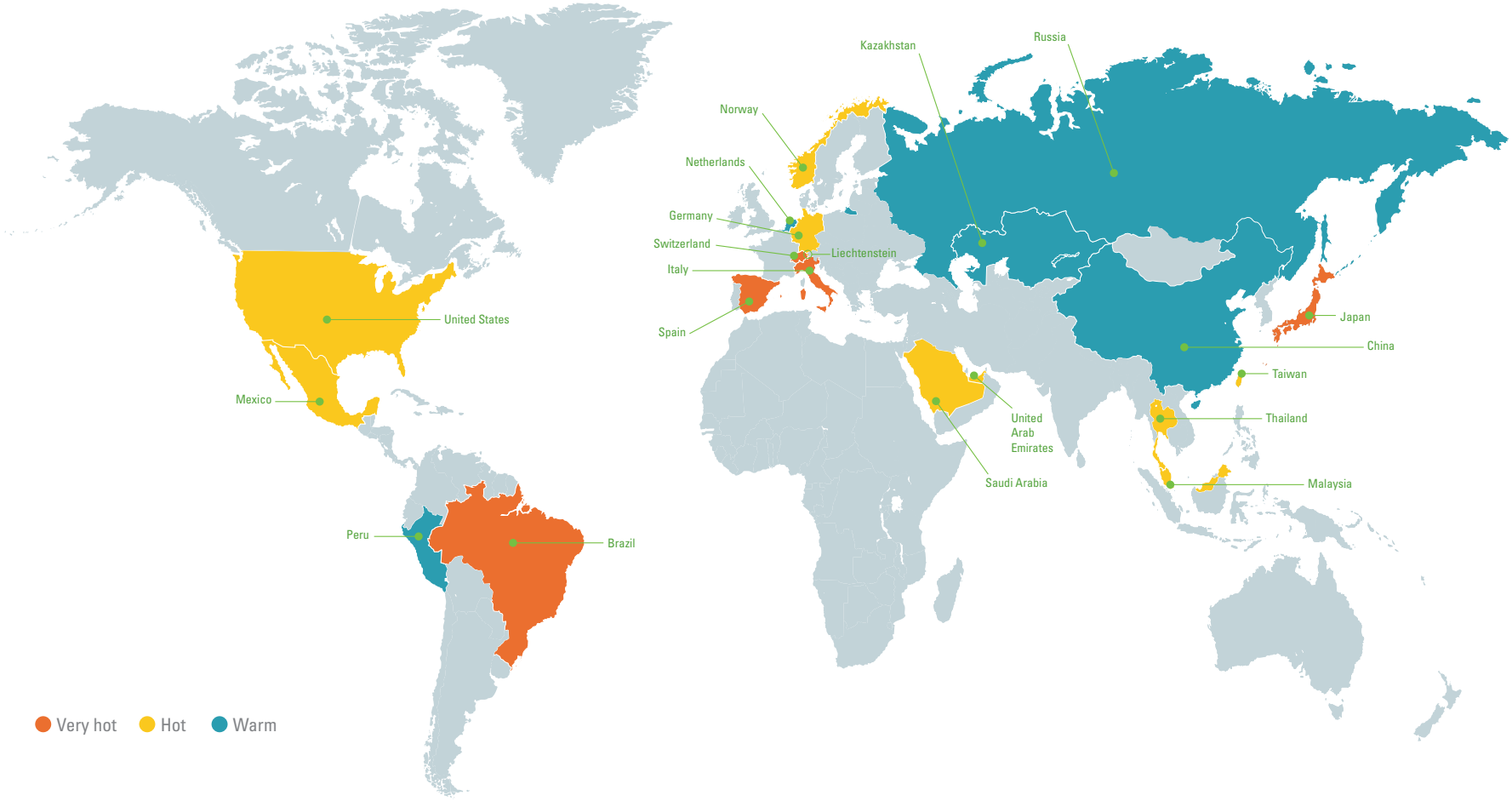


Figure 2

Heat-map of information leaking countries



Collecting **Meta-Data**

78%

OF FORBES 2000 CORPORATE WEBSITES LEAK SOME FORM OF POTENTIALLY USEFUL INFORMATION THROUGH DOCUMENT META-DATA

Information within document meta-data often constitutes an information leak as it can provide cyber attackers with a view of corporate network users, their email addresses, the software versions they use to create documents and internal network locations where files are stored.

KPMG downloaded almost 10 million publicly-available documents across the Forbes 2000 corporate websites including common file types such as Microsoft Office and Adobe Acrobat PDF. Once downloaded, automated tools were used to extract meta-data from these files, such as the username of the creator, the network location where the document was created or saved and the version of software used to create the document.

By sector, the distribution shows that technology and software sectors appear to expose the most information in relation to the meta-data in documents they serve on their corporate websites.

This part of the research quickly demonstrated the ease with which cyber attackers can target specific individuals and the vulnerable software versions that they may be using on their computers. Sadly, it is relatively straightforward to visit a hacking website, pay US$200 and have a bespoke Trojan email produced, specifically targeted at one individual within a company. If the target of these attacks is lucky, their spam filter will block the email, if not then their corporate secrets may be revealed upon a seemingly innocent click of a button.

The following meta-data information leaks were collected across all Forbes 2000 corporate websites:

Information leak	Total across all 2000 sites	Average per site
Number of potential usernames	419,430	210
Number of network folders and locations	104,370	52
Number of printers and their hostnames	33,250	17
Number of software applications and versions	70,910	35
Number of email addresses	342,040	171

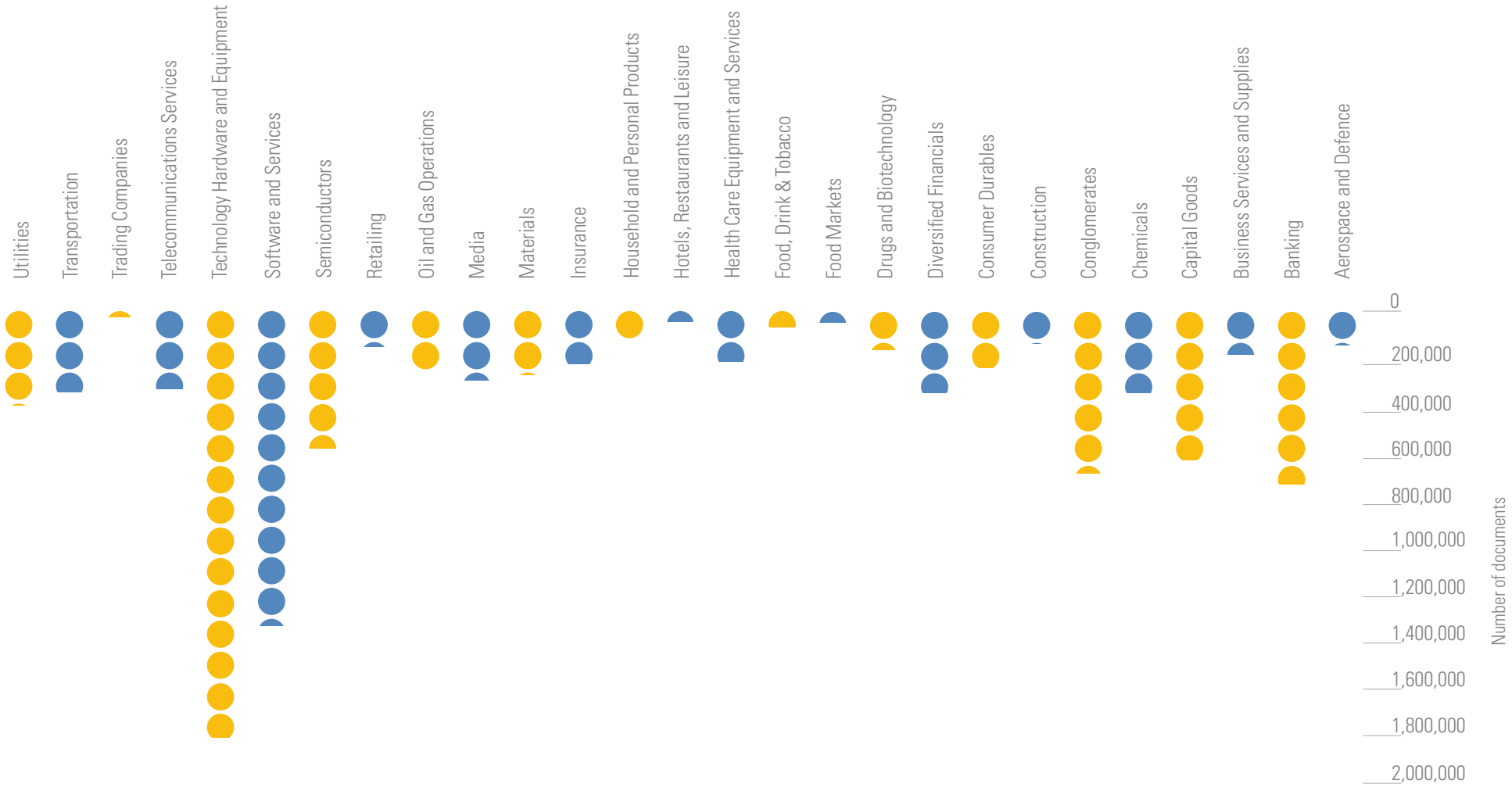
Figure 3. Meta-data information leaks across all sites

What is meta-data?

Document meta-data is information 'about' a document, or information on its properties. It often informs who created a document, when and where on a device or network.

Figure 4

Number of documents on corporate websites by sector



Harvesting **Sensitive Locations** and **Hidden Functionality**

15%

OF THE FORBES 2000 CORPORATE WEBSITES OFFER HACKERS ACCESS TO TEST FUNCTIONALITY AND PRIVATE LOGIN PORTALS THAT POTENTIALLY ALLOW FILE UPLOAD CAPABILITIES

Part of our research focussed on the structure of the Forbes 2000 corporate websites to identify any potentially sensitive file locations or hidden functionality that may be useful to cyber attackers. While navigating the sites, we found a number of keywords that revealed interesting file locations that would stimulate further investigation by cyber attackers (see Figure 5).

A large number of temporary files were found across the sites, in addition to administrative and private login portals for webmasters. Upload functionality was discovered on some sites which might enable cyber attackers to upload software to execute commands on those web servers. Backup and test content, providing enhanced functionality over the corporate websites, was also discovered in many instances.

A number of file locations marked 'private' were also identified, hosting documents that were not intended for public consumption. In particular, Banking, Diversified Financials and Insurance companies seem to be exposing sensitive information and hidden functionality on their websites (see Figure 6).

Figure 5
Top 10 keywords revealing interesting file locations on corporate websites

Keyword	Number of Occurrences	Description
Temp	553	Temporary files sometime revealing test information
Data	481	Sometimes data folders including backup client or corporate data
.txt	429	Many text files found with system configuration information
Test	293	Website test functionality, sometimes providing enhanced functionality on websites
Admin	292	Administrative pages, often protected with a login
Login	246	Sometimes included login for site management and content modification
Private	233	Some files available which perhaps should be protected
Upload	111	Some instances of remote file upload capabilities
Secure	87	Often protected by a login, but highlighting areas of possible interest by attackers
Command	59	Some instances of potential to run commands on the web server

Hacker alert!

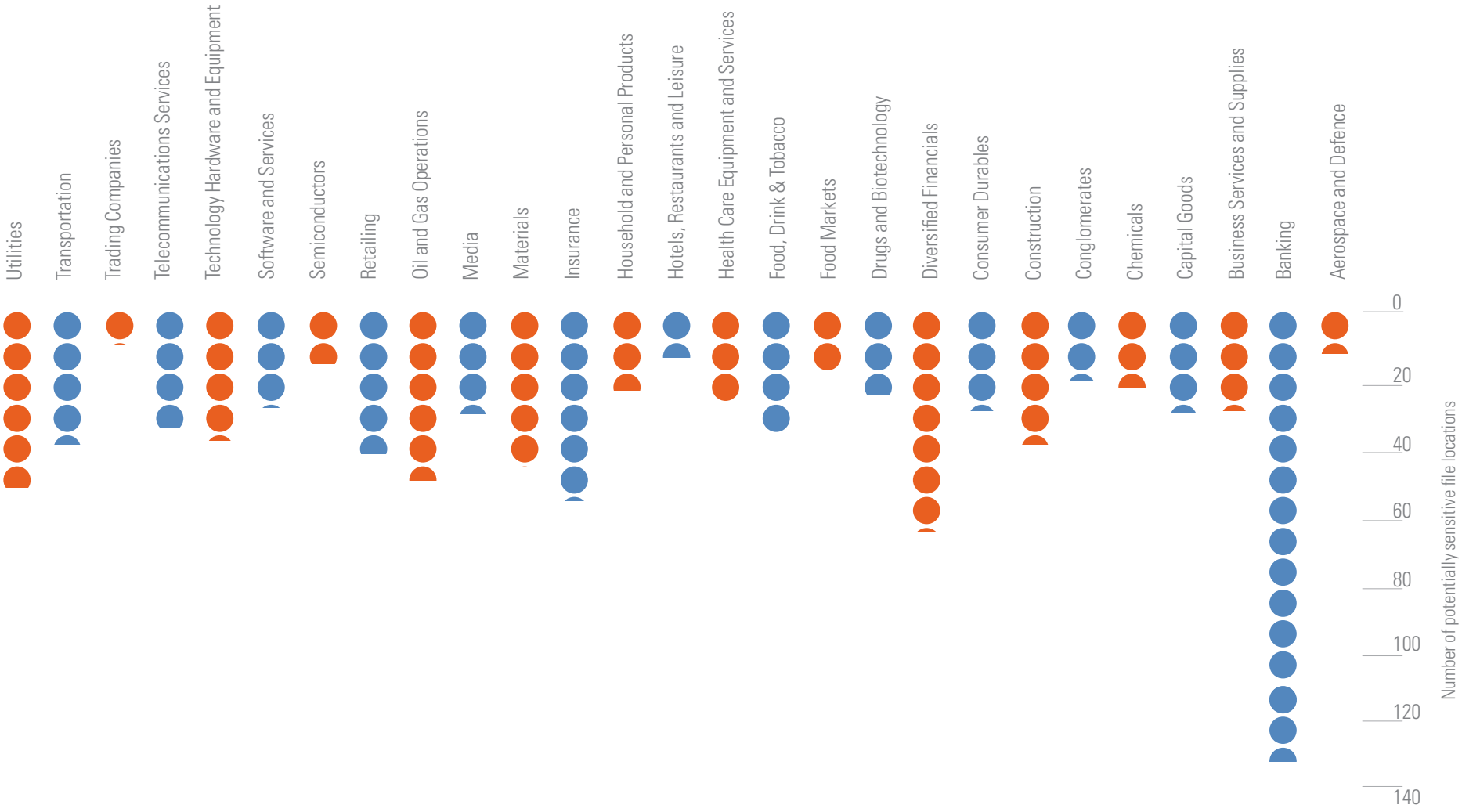
US Cyber Security response team warn of attacks upon the gas industry

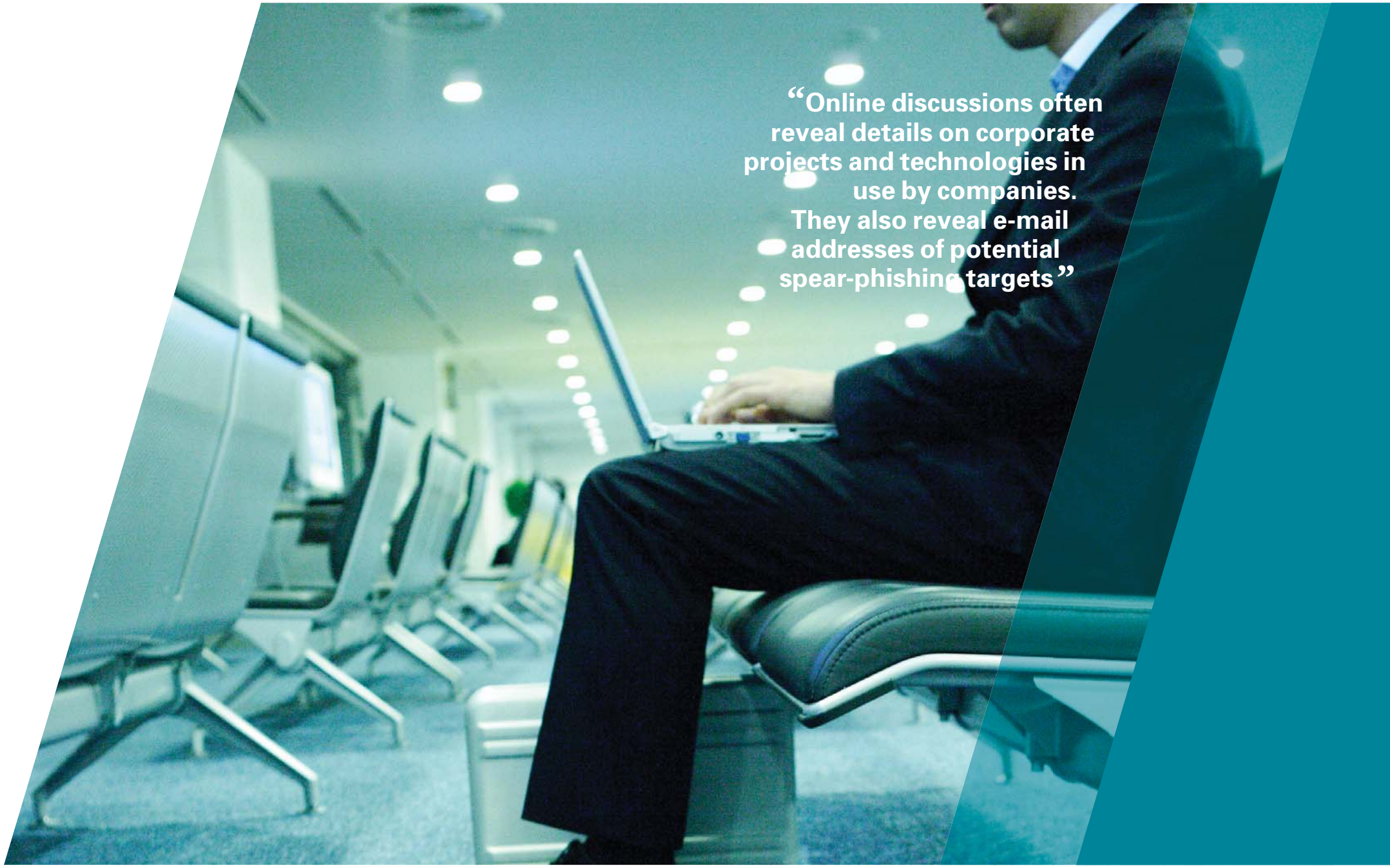
April 2012, ICS-CERT reported a number of cyber intrusions targeting gas pipeline companies. Analysis of the attacks confirm they are part of an ongoing campaign dating back to December 2012 and confirm Spear-phishing was used to target a number of specific individuals acrossthe gas pipeline industry.

When serving test, upload or hidden functionality, many companies face the associated risk of cyber attackers defacing websites, or assuming control of these sites. Cyber attackers may also use this newly gained functionality to inject malware into the sites which will infect all subsequent visitors of those sites.

Figure 6

Number of potentially sensitive file locations on the Forbes 2000 corporate websites by sector





Gathering **Data** from Popular **Search Engines**

COMPANIES INVOLVED IN TECHNOLOGY AND SOFTWARE POST FAR MORE INFORMATION TO ONLINE FORUMS AND NEWSGROUPS THAN ALL OTHER SECTORS COMBINED

As part of many popular search engine services, discussions are stored within a searchable web cache and can be queried for specific postings by users. In addition to the meta-data available, individuals often expose within these postings sensitive information about the current technologies in use by organisations.

We found that technology and software companies post far more information to online forums and newsgroups than all other sectors combined.

For this portion of the research, we queried a popular search engine's postings written by individuals with email addresses at Forbes 2000 organisations. We found that, on occasion, what might be deemed commercially-sensitive information was found posted to public domain forums. The top 10 organisations in terms of number of postings in such forums included members of the technology, software and semiconductor and telecommunication industries.

Figure 7
Top 10 sectors posting the most information to public forums and newsgroups.

Sector	Number of newsgroup postings
Software & Services	49,965,680
Telecommunications Services	1,239,827
Technology Hardware & Equipment	769,574
Semiconductors	237,791
Conglomerates	193,118
Media	170,634
Aerospace & Defence	146,751
Drugs & Biotechnology	100,178
Oil & Gas Operations	88,681
Banking	88,527

Hacker alert!

Cyber attackers will spend time trawling newsgroups for information relating to potential targets. These postings often reveal email addresses of individuals to be targeted in spear-phishing attacks, and may also reveal information on an individual's hobbies, interests or specific work areas which can be used in targeted social engineering attacks.

"Many instances of un-patched and unsupported web server software were found to be serving some Forbes 2000 corporate websites"

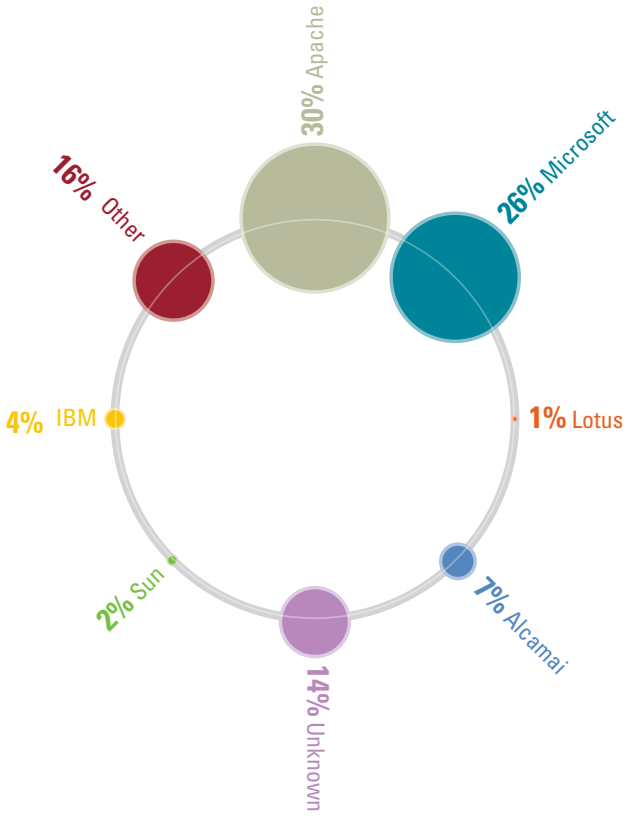
Web Server Software **Vulnerabilities**

16%

OF FORBES 2000 CORPORATE WEB SERVERS MAY BE VULNERABLE TO ATTACK DUE TO MISSING SECURITY PATCHES OR OUT-DATED SERVER SOFTWARE

Figure 8

Web server technologies across the Forbes 2000 corporate websites



As part of our research, our security experts identified the specific web server technologies used across corporate sites (see Figure 8), and correlated this data against known security flaws, to identify the 10 sectors vulnerable in terms of their underlying web server technology. Of the two most common software systems in use by corporations, 8 percent of Apache web servers were found to be potentially vulnerable, and 6 percent of Microsoft web servers were potentially vulnerable.

Looking at the results across industry groups (see Figure 9), Utilities stand out as the most vulnerable sector affected by version issues of their web server software.

We also explored web server software security on a country basis; this revealed that a number of countries are further behind others with regards to software vulnerability patching and updating of their web servers (see Figure 10).

Hacker alert!

Any web server on the Internet running un-patched versions of web server software is vulnerable to remote attack – the result of a successful attack could range from a Denial of Service (DoS) attack on the website, to the attacker gaining full control of the web server and its content.

Corporate websites run on an underlying web server technology. When accessing a website the web server often reveals its software version which is typically hidden from a web browser's view. Information leakage in these web banner software versions can prove to be of significant value to an attacker when profiling a remote target site and server.

Figure 9

Number of potential vulnerabilities affecting corporate web servers per sector

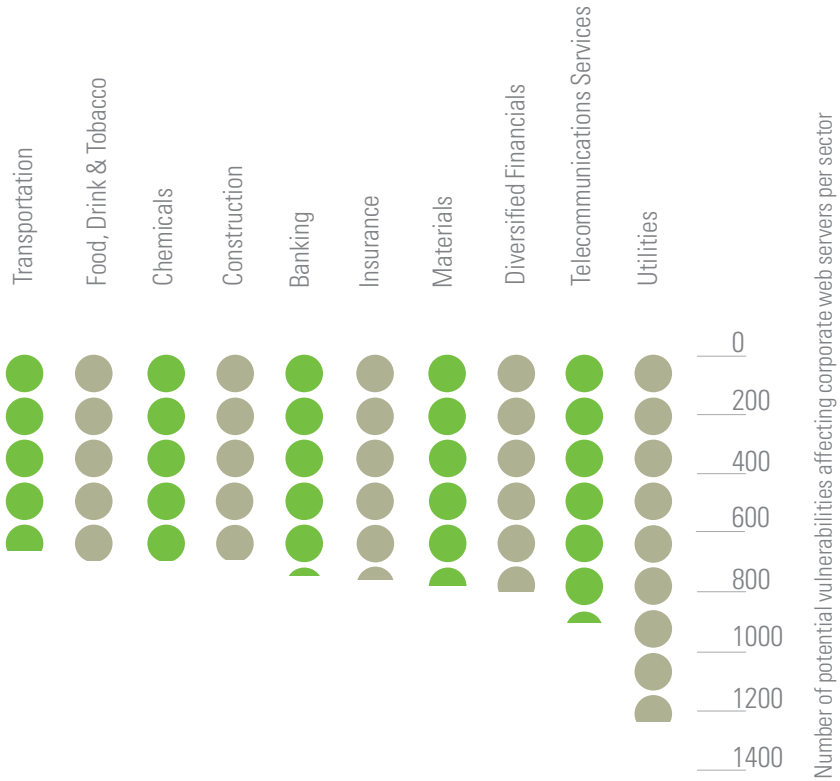
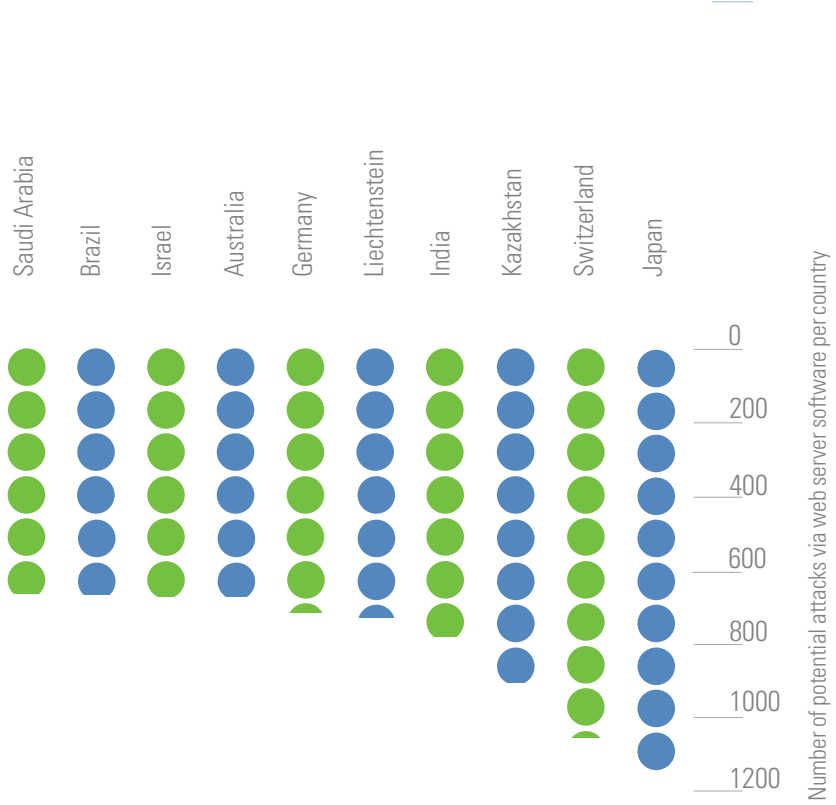


Figure 10

Top 10 countries vulnerable to potential attack via vulnerable web server software



“The most information leaks by sector affect Financial Services, Software, Technology, Telecoms and Banking organisations”

Who is **Most** at **Risk?**

THE TOP 10 FORBES 2000 COMPANIES LEAKING INFORMATION HAIL FROM EITHER THE US OR JAPAN. MOST OF THESE ORGANISATIONS ARE IN SOFTWARE OR TECHNOLOGY-RELATED SECTORS

Cyber attackers and organised crime do not only target one avenue of attack. Instead, they use a combination of available information leaks to profile a target, and map them out their internal systems and their components.

Cyber attackers will devote time and effort in profiling the entire online presence of potential targets; as a result, the more information volunteered about a system or network, the more likely an attacker might be to further explore potential avenues of attack.

It is important to emphasise that the processes used to gather the information leaks for our research were not sophisticated and are available to anyone with access to the Internet and little more than a web browser.

To conclude our research, we aggregated all normalised data from the overall information leakage survey on a per company, per sector and per country basis, revealing clear tends. Correlation of all results revealed that, across the Forbes 2000 list of companies, the greatest number of information leaks affect financial, software, technology and telecoms sectors. Indeed, the banking sector in particular seemed most exposed.

However, technology and software sectors also seem to be at risk with employees within these sectors appearing to publish much information in the form of documents and online forum queries. As such, these sectors are at risk of inadvertent exposure of sensitive information relating to their technologies and intellectual property.

While the per country figures demonstrate the extent of the challenge being faced around the world, there are a number of countries (Japan and Switzerland in particular) that seem to be more exposed.

We took the additional step of collating the results to identify the 10 Forbes 2000 companies that offered cyber attackers the most opportunity.

The names of the Top 10 at risk organisations shall remain anonymous, however our summary of these organisations shows the sector to which they belong and the country in which they operate. The magnitude of each bar represents the amount of information leaked by that organisation (see Figure 13).

Figure 11

Top 10 information leaking sectors

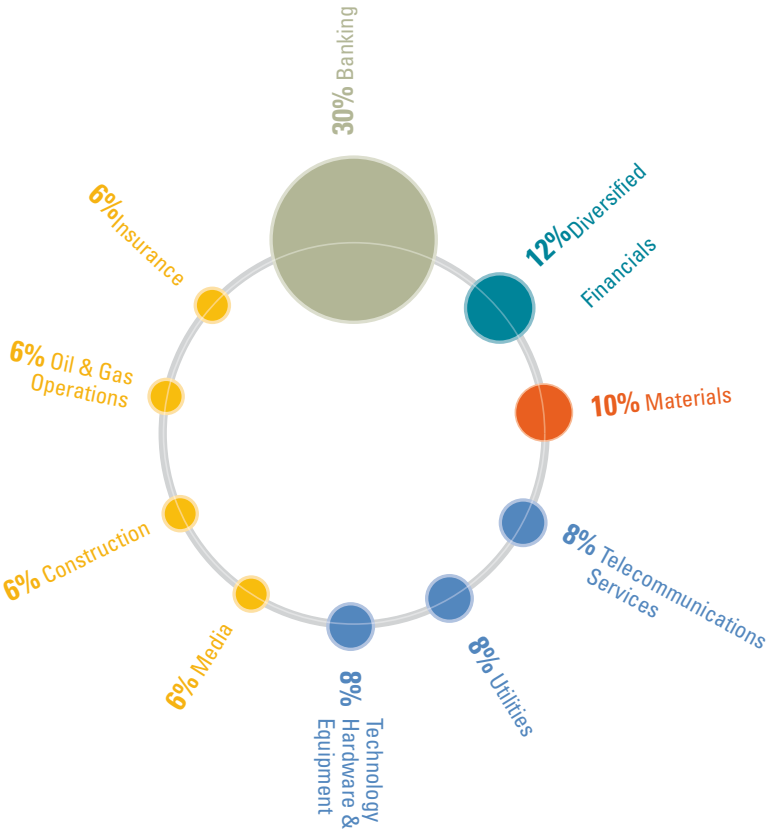


Figure 12

Top 10 information leaking countries

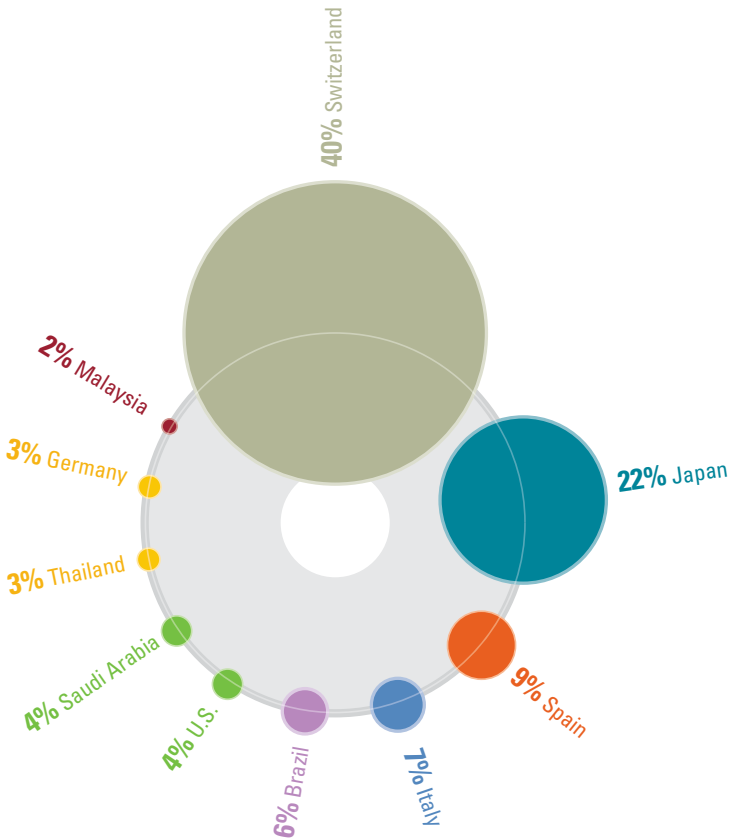
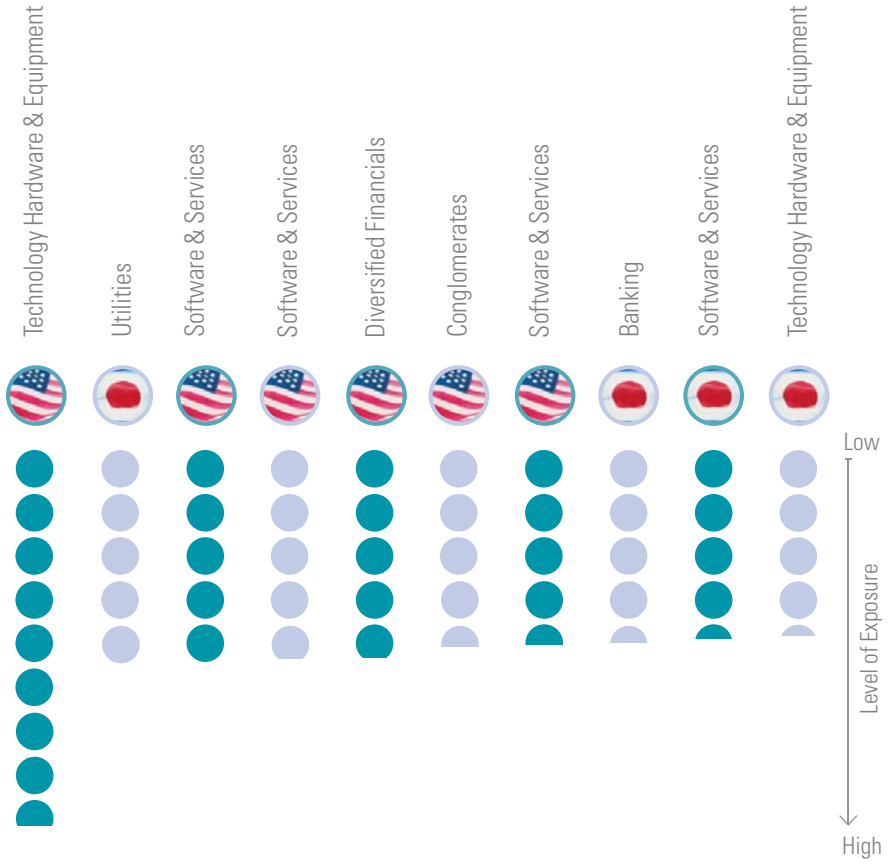


Figure 13

Top 10 exposed organisations by sector and operating country



4 Steps to Minimise your Exposure

The world of cyber security has tilted on its axis. Companies now not only face cyber attacks from hacking groups, script kiddies and hactivists but also from state-sponsored agencies with limitless resources, seeking a competitive edge or intellectual property. Just as attacks have evolved companies must evolve by re-evaluating their own ability to detect, defend and respond to cyber attacks.

The types of information gained as part of our research are proven to have been of use in real-world cyber attacks. KPMG's Cyber Response team has successfully penetrated organisational defences and perimeters using such information leaks, as part of legitimate client engagements around social engineering and ethical hacking.

Whilst each company must perform a bespoke risk assessment against their own digital estate, the following steps will go some way to improve cyber security and reduce the amount of extraneous meta-data which companies expose on the Internet.

01

ASSESS

Perform an assessment of your Internet presence. What data does your organisation currently leak to the world?

02

SPRING CLEAN

Where possible, cleanse meta-data from your existing published documents. Ensure all corporate devices are fully patched, not just your online web servers.

03

EDUCATE "ALL" EMPLOYEES

Everyone in the organisation – from the boardroom to the mailroom – must understand the value and sensitivity of the information they possess and, more importantly, how to protect it.

04

ADJUST POLICIES

Instigate a policy to minimise unintentional or undesired corporate information appearing on the Internet.

Cyber Response methodology

BENCHMARKING

We can assess your company's Internet profile and benchmark performance against industry peers.

TESTING

We can perform simulated cyber attacks and social engineering exercises against your infrastructures to identify your existing exposure and failures in existing security controls and processes.

REMEDIATION

If your company falls below industry peers, we can initiate remediation programmes to identify any gaps and instigate improvement programmes.

KPMG

We have a comprehensive Cyber Response methodology and service which covers all facets of proactive and reactive cyber response:

- Prepare and Train
- Detect and Initiate
- Contain and Investigate
- Report and Improve

POLICING

We can deploy a service to continuously monitor your presence on the Internet.

Glossary of terms

Apache
Open source web server software

APT
Advanced Persistent Threat (APT) is characterised by the covert penetration of systems by unauthorised individuals to illegally exfiltrate information of political, military or economic value from an organisation over a sustained period of time, typically using information for competitive advantage. Initial attacks may be a precursor to later attacks on the same organisation or used as a stepping stone to attack another organisation

Backdoor
A method of gaining persistent access to resources which typically by passes security controls

Denial of Service (DoS)
Attacks involving attempts to render IT resources unavailable or unusable by legitimate users

File Upload
Functionality which allows for files and documents to be uploaded over the Internet to a remote website or server

ICS - CERT
Industrial Control Systems Cyber Emergency Response Team

Malware
Malicious software, deliberately written with malicious intent, to gain unauthorised access or cause damage to computers and networks

Meta-Data
Information within a document 'about' the document and its properties

Microsoft™ IIS
Closed source web server software by Microsoft

Script kiddies
a young person with limited technical skills who uses programs developed by more technical individuals to attack networks and websites

Social Engineering
Process of manipulating or fooling individuals into divulging information

Vulnerability
A weakness or flaw in a system or process that if exploited might result in a compromise of resources

Contact us

Malcolm Marshall
Partner, Head of Information Protection and Business Resilience
+44 (0)20 7311 5456
malcolm.marshall@kpmg.co.uk

Stephen Bonner
Partner, Financial Services, Information Protection and Business Resilience
+44 (0)20 7694 1644
stephen.bonner@kpmg.co.uk

Charles Hosner
Partner, Corporates, Information Protection and Business Resilience
+44 (0)7500 809 597
charles.hosner@kpmg.co.uk

Martin Jordan
Head of Cyber Response
+44 (0)776 846 7896
martin.jordan@kpmg.co.uk

www.kpmg.co.uk/security

About us

KPMG Risk Consulting brings together specialists with skills focussed on the Information and Technology Risk agenda. We have a team of over 3,500 professionals advising clients across all markets and geographies of the technology and data risks they face. We are a global network of KPMG member firms with over 140,000 professionals in 150 countries.

We help our clients to prevent, identify and remediate Information and Technology failures and ensure systems are fit for the future. Our independent advice and advanced technology capabilities help our clients manage their technology risks and use their data to its full potential.

Our award winning Information Protection team helps organisations assess risk and design, test, and implement the controls required to protect them from security breaches, including accidents and cyber attack.

KPMG's UK Cyber Response team is comprised of experienced, highly technical security consultants. The team is proficient in penetrating client IT systems in order to identify security weakness in their infrastructures and to articulate the security risks to their business, alongside practical mitigation advice. We are also specialists in responding to cyber incidents and help clients effectively manage their response to cyber attack through detection, containment, recovery and Cyber Response improvement programmes.

Why us

- Award-winning – KPMG was awarded 'Information Security Consultant of the Year 2012' at the SC Magazine Europe Awards 2012. This is the second year running that KPMG has won the award. KPMG were also highly commended for the Information Security Project of the Year category for I-4 programme, which is the leading information security forum for large global businesses. Our Information Protection team also received the 2010 Management Consulting Association (MCA) Management Award for Business Strategy for our work with a leading bank on a major third-party security assurance programme.
- Commitment - KPMG's client relationships are built on mutual trust and long-term commitment to providing effective and efficient solutions. We are dedicated to providing a service that is second to none.
- Industry knowledge - Through I-4 (the International Information Integrity Institute) we help the world's leading organisations to work together to solve today's and tomorrow's biggest security challenges. To learn more go to www.i4online.com

RR Donnelley I RRD-270670 I July 2012