Alan Ryan
alan.ryan@netinsight.net

Cyber Security for business

MTI and Alan Ryan at a glance

Providing data securely for 25+ years across public, social and private market sectors.

30 years in the industry (Me)

World class sales, service & consulting organisation

24x7x365 global **Secure Operations Centre** (SOC)

Vendor trained professional services team and a highly qualified pen testing division accredited for public and private sector work.

2000+ PS/PEN days delivered p.a.

Objectives

Agenda

- Cybersecurity
    - Background
    - Today's attacks
    - Data Breaches and their causes

    - Big business vs small businesses
        - Why they are both targets

    - Investment in Cybersecurity

    - The problem that cannot be solved

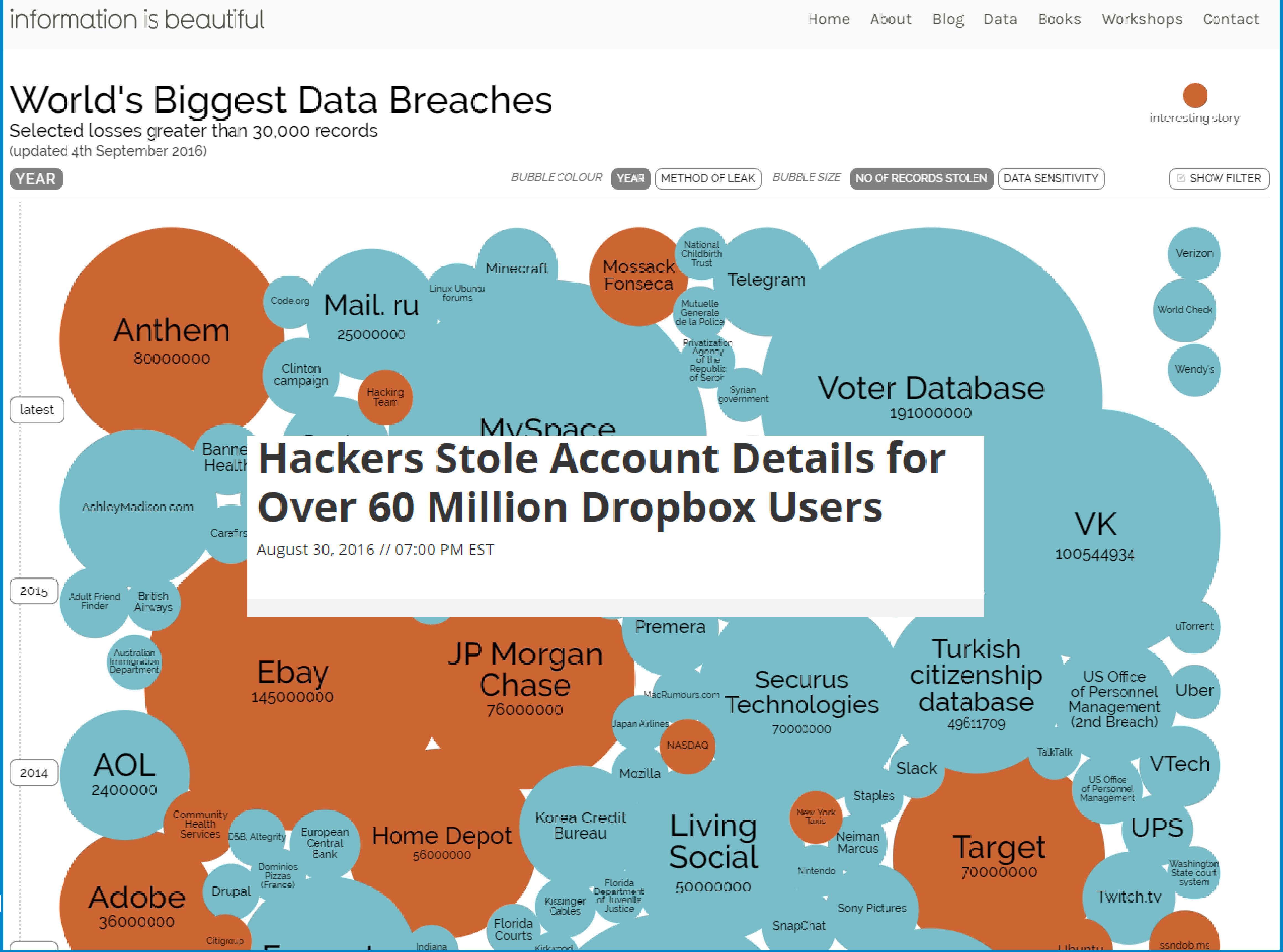
    - Visibility, coverage and response
        - A practical approach mitigating risk and obtaining budget
        - Prioritising resources

    - GDPR

There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



information is beautiful

Home About Blog Data Books Workshops Contact

World's Biggest Data Breaches

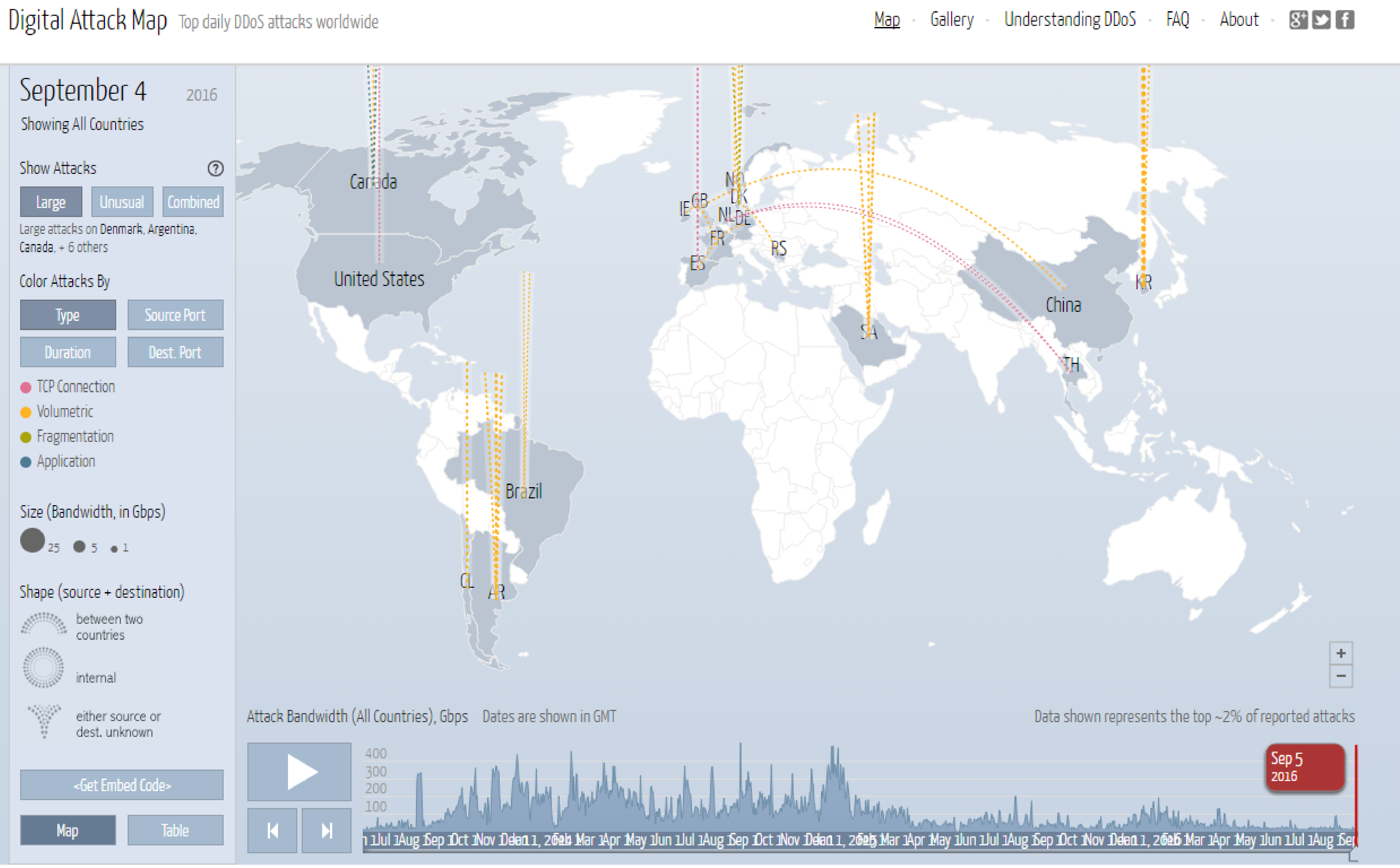
Selected losses greater than 30,000 records

(updated 4th September 2016)

Hackers Stole Account Details for Over 60 Million Dropbox Users

August 30, 2016 // 07:00 PM EST

http://www.digitalattackmap.com/



Digital Attack Map Top daily DDoS attacks worldwide

September 4 2016

Showing All Countries

Show Attacks

Large attacks on Denmark, Argentina, Canada, + 6 others

Color Attacks By

● TCP Connection
● Volumetric
● Fragmentation
● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

Shape (source + destination)

between two countries

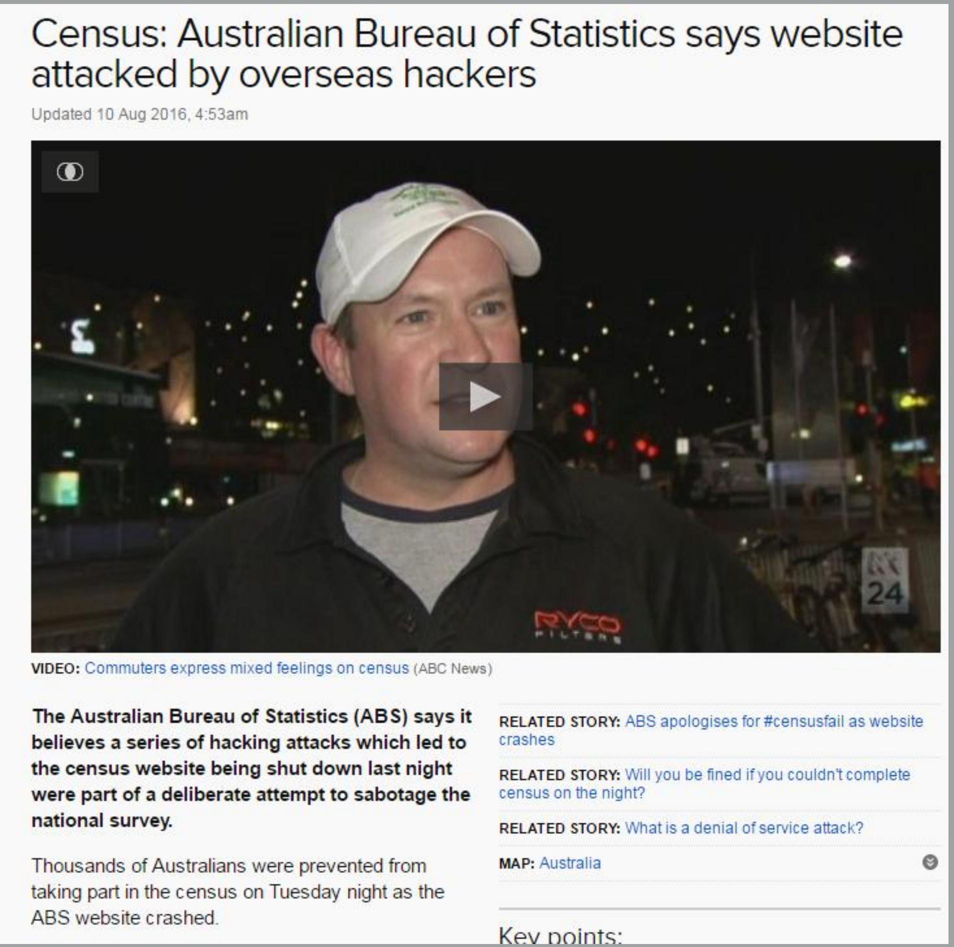
internal

either source or dest. unknown

Attack Bandwidth (All Countries), Gbps Dates are shown in GMT

Data shown represents the top ~2% of reported attacks

400
300
200
100
Jul Aug Sep Oct Nov Dec Jan 1, 2014 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 1, 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 1, 2016 Feb Mar Apr May Jun Jul Aug Sep
Sep 5
2016



Census: Australian Bureau of Statistics says website attacked by overseas hackers

Updated 10 Aug 2016, 4:53am

VIDEO: Commuters express mixed feelings on census (ABC News)

The Australian Bureau of Statistics (ABS) says it believes a series of hacking attacks which led to the census website being shut down last night were part of a deliberate attempt to sabotage the national survey.

Thousands of Australians were prevented from taking part in the census on Tuesday night as the ABS website crashed.

RELATED STORY: ABS apologises for #censusfail as website crashes

RELATED STORY: Will you be fined if you couldn't complete census on the night?

RELATED STORY: What is a denial of service attack?

MAP: Australia

Key points:

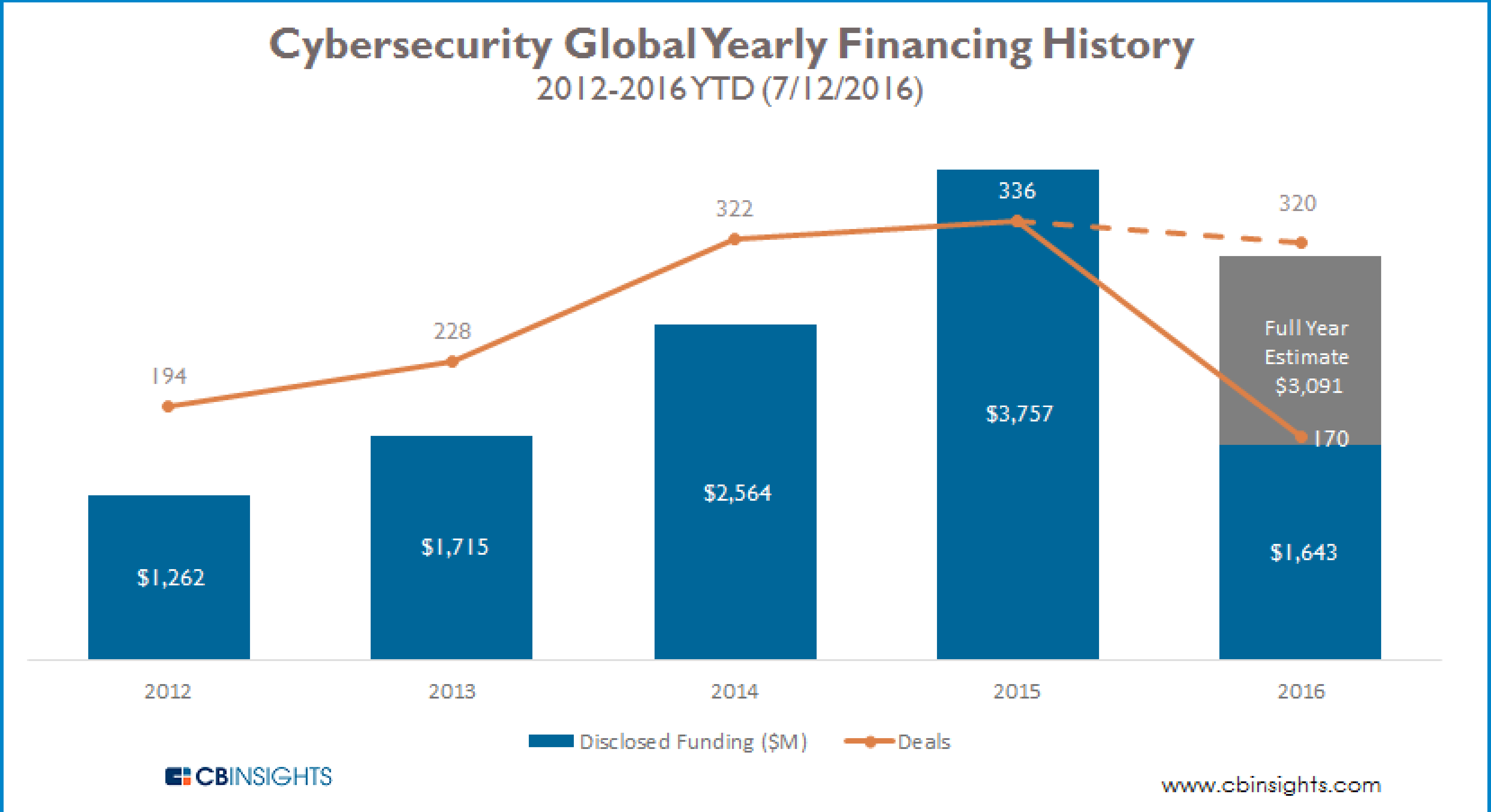
Hackers take control of systems and computers in order to launch DDoS attacks (Distributed Denial of Service). This is the same form of attack used against the Austrailian Bureau of Statistics Census a few months ago. The attacks to Newsat were the worst they had ever seen.

“Our network was, as far as they could see, the most corrupted they had ever seen,” former CFO of Newsat Michael Hewins said.

Newsat used to be Australia’s largest satellite company and had plans for launching two satellites to kickstart the industry in Austrailia. After the cyber-attacks, liquidators were called in to sell off all of the assets that were left.

Hiring a DDOS attack

2015 - $38 per hour
2016 - $5 an hour



Cybersecurity Global Yearly Financing History

2012-2016 YTD (7/12/2016)

SecurEnvoy

hp

Blue Coat®

McAfee®

SOPHOS

WatchGuard™

websense®
ESSENTIAL INFORMATION PROTECTION™

CISCO™

IBM

f5®

riverbed®

RSA
SECURITY®

Microsoft®

SafeNet™

celestix

TREND MICRO™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Symantec

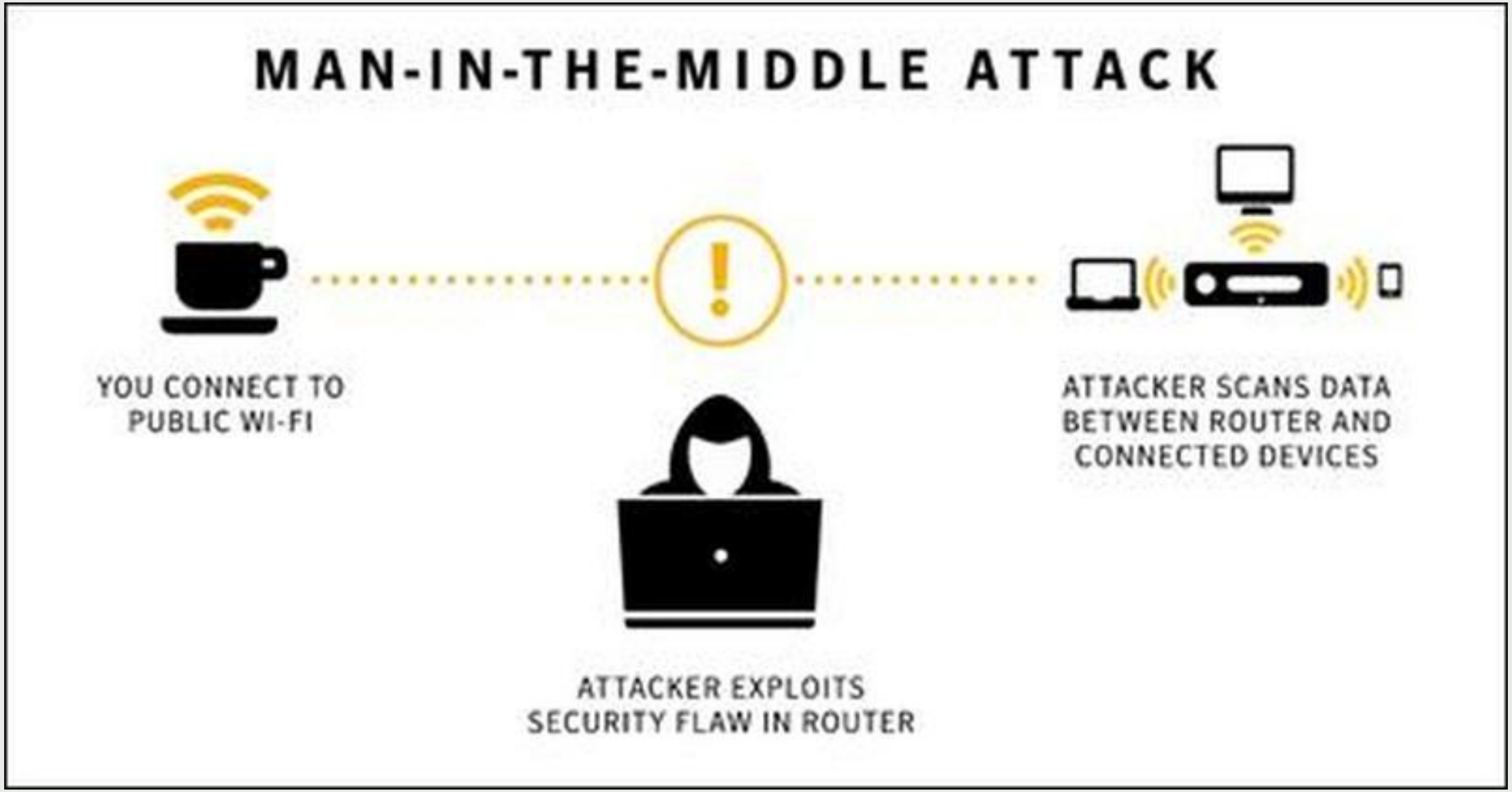
Juniper®
NETWORKS

FORTINET®

WHY IS THIS HAPPENING?

- The traditional boundary does not exist
  - No single egress and ingress point
    - Mobile devices, cloud services, third-parties
- Criminals are extremely patient and sophisticated
  - APT, phishing, DDoS costs
- Mistakes happen, human intervention is required in too many cases
- Public Wifi – man in the middle attacks

Man in the middle

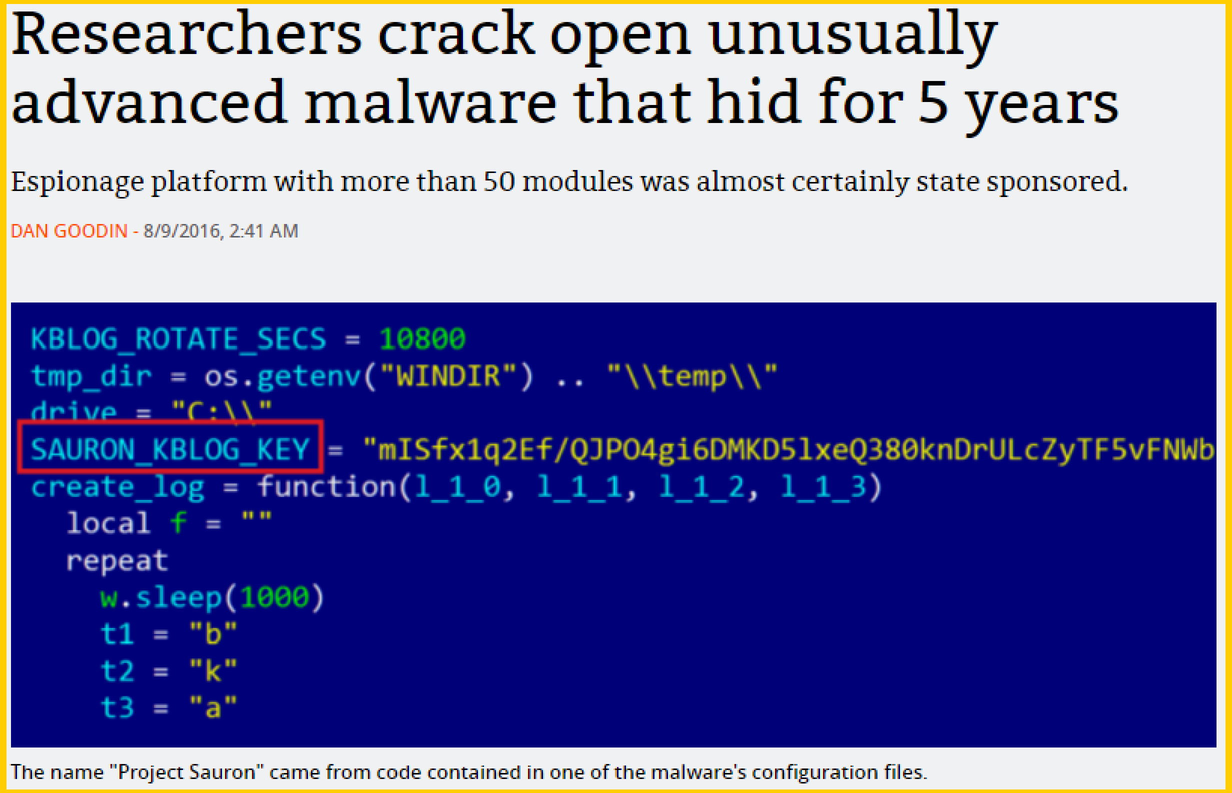

MAN-IN-THE-MIDDLE ATTACK
YOU CONNECT TO PUBLIC WI-FI
ATTACKER EXPLOITS SECURITY FLAW IN ROUTER
ATTACKER SCANS DATA BETWEEN ROUTER AND CONNECTED DEVICES

1. Use a VPN
2. Use SSL
3. Turn off sharing
4. Use and disconnect

SecurEnvoy
hp
Blue Coat
McAfee
SOPHOS
WatchGuard
websense
ESSENTIAL INFORMATION PROTECTION
CISCO
IBM
f5
RSA
SECURITY
Microsoft
riverbed
SafeNet
celestix
TREND MICRO
Check Point
SOFTWARE TECHNOLOGIES LTD.
Symantec
Juniper
NETWORKS
FORTINET

APT’s Sandboxing

Sandboxing?



Researchers crack open unusually advanced malware that hid for 5 years

Espionage platform with more than 50 modules was almost certainly state sponsored.

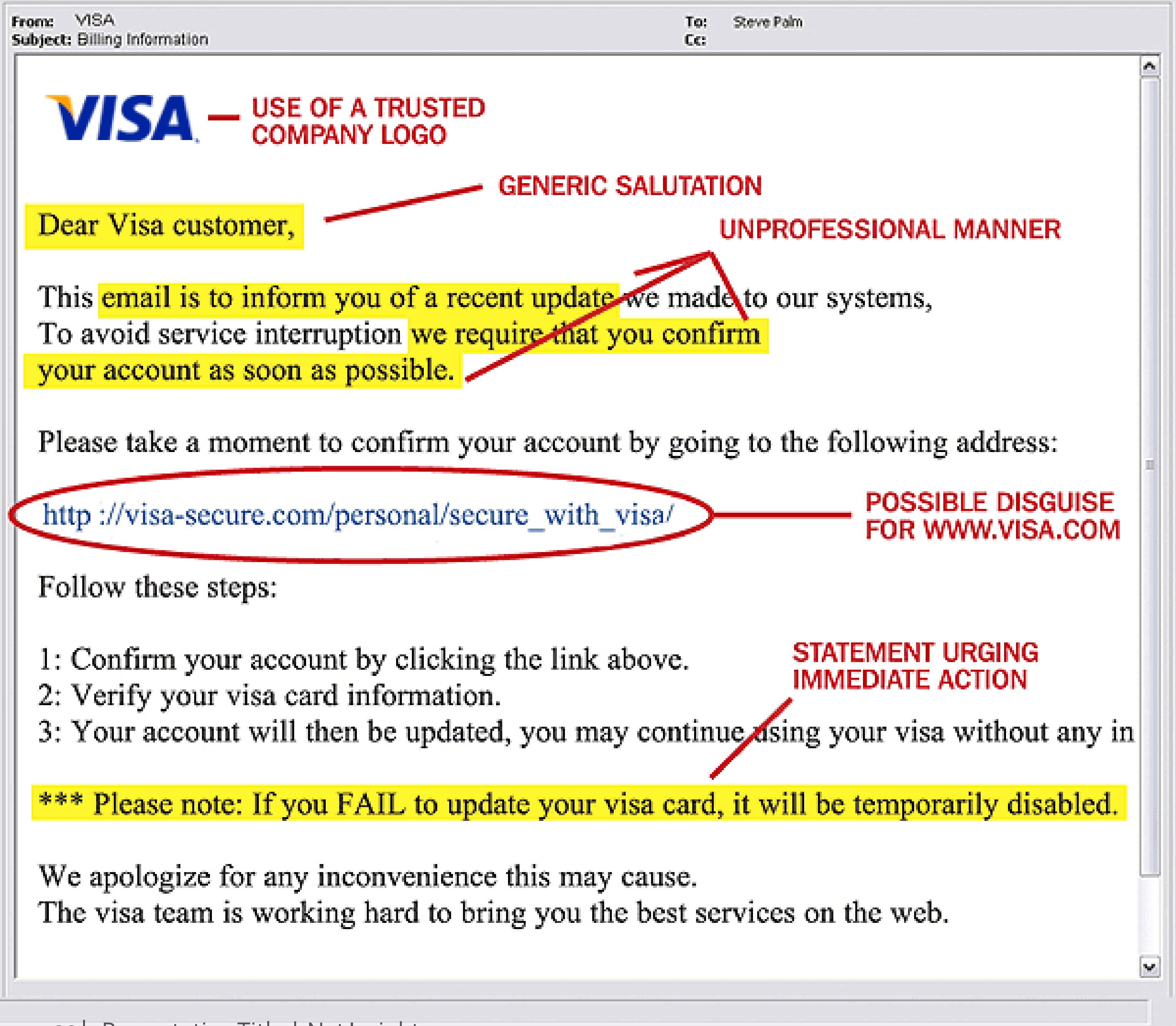
DAN GOODIN - 8/9/2016, 2:41 AM

```
KBLOG_ROTATE_SECS = 10800
tmp_dir = os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD5lxeQ380knDrULcZyTF5vFNWb
create_log = function(l_1_0, l_1_1, l_1_2, l_1_3)
  local f = ""
  repeat
    w.sleep(1000)
    t1 = "b"
    t2 = "k"
    t3 = "a"
```

The name "Project Sauron" came from code contained in one of the malware's configuration files.

Phishing

Philshing



From: VISA
Subject: Billing Information
To: Steve Palm
Cc:

VISA — USE OF A TRUSTED COMPANY LOGO

GENERIC SALUTATION

Dear Visa customer,

UNPROFESSIONAL MANNER

This email is to inform you of a recent update we made to our systems,
To avoid service interruption we require that you confirm
your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

http ://visa-secure.com/personal/secure_with_visa/

POSSIBLE DISGUISE FOR WWW.VISA.COM

Follow these steps:

STATEMENT URGING IMMEDIATE ACTION

1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

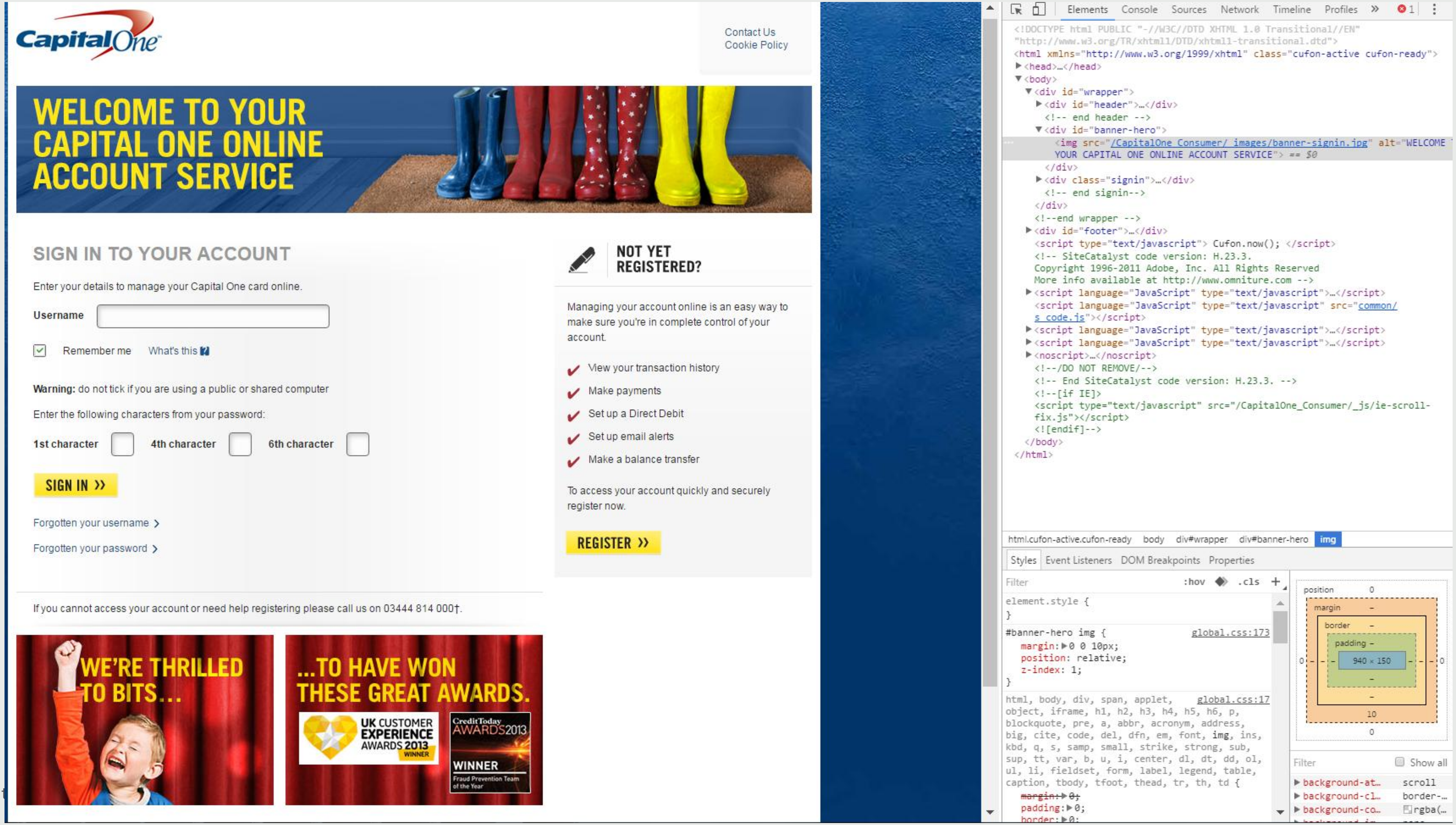
We apologize for any inconvenience this may cause.
The visa team is working hard to bring you the best services on the web.

- Training for staff
  - Emails from non listed suppliers

•Spam filters are better

•Look at email addresses

Philshing



Contact Us
Cookie Policy

WELCOME TO YOUR CAPITAL ONE ONLINE ACCOUNT SERVICE

SIGN IN TO YOUR ACCOUNT

Enter your details to manage your Capital One card online.

Username

☑ Remember me What's this

Warning: do not tick if you are using a public or shared computer

Enter the following characters from your password:

1st character □ 4th character □ 6th character □

SIGN IN »

Forgotten your username ›

Forgotten your password ›

If you cannot access your account or need help registering please call us on 03444 814 000†.

NOT YET REGISTERED?

Managing your account online is an easy way to make sure you're in complete control of your account.

- ✓ View your transaction history
- ✓ Make payments
- ✓ Set up a Direct Debit
- ✓ Set up email alerts
- ✓ Make a balance transfer

To access your account quickly and securely register now.

REGISTER »

WE'RE THRILLED TO BITS...
...TO HAVE WON THESE GREAT AWARDS.
UK CUSTOMER EXPERIENCE AWARDS 2013 WINNER
CreditToday AWARDS 2013
WINNER
Fraud Prevention Team of the Year
Elements
Console
Sources
Network
Timeline
Profiles
1

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" class="cufon-active cufon-ready">
▶<head>…</head>
▼<body>
  ▼<div id="wrapper">
    ▶<div id="header">…</div>
     <!-- end header -->
    ▼<div id="banner-hero">
       <img src="/CapitalOne_Consumer/_images/banner-signin.jpg" alt="WELCOME 
       YOUR CAPITAL ONE ONLINE ACCOUNT SERVICE"> == $0
     </div>
    ▶<div class="signin">…</div>
     <!-- end signin-->
   </div>
   <!--end wrapper -->
  ▶<div id="footer">…</div>
   <script type="text/javascript"> Cufon.now(); </script>
   <!-- SiteCatalyst code version: H.23.3.
   Copyright 1996-2011 Adobe, Inc. All Rights Reserved
   More info available at http://www.omniture.com -->
  ▶<script language="JavaScript" type="text/javascript">…</script>
   <script language="JavaScript" type="text/javascript" src="common/
   s_code.js"></script>
  ▶<script language="JavaScript" type="text/javascript">…</script>
  ▶<script language="JavaScript" type="text/javascript">…</script>
  ▶<noscript>…</noscript>
   <!--/DO NOT REMOVE/-->
   <!-- End SiteCatalyst code version: H.23.3. -->
   <!--[if IE]>
   <script type="text/javascript" src="/CapitalOne_Consumer/_js/ie-scroll-
   fix.js"></script>
   <![endif]-->
 </body>
</html>
```

html.cufon-active.cufon-ready body div#wrapper div#banner-hero img

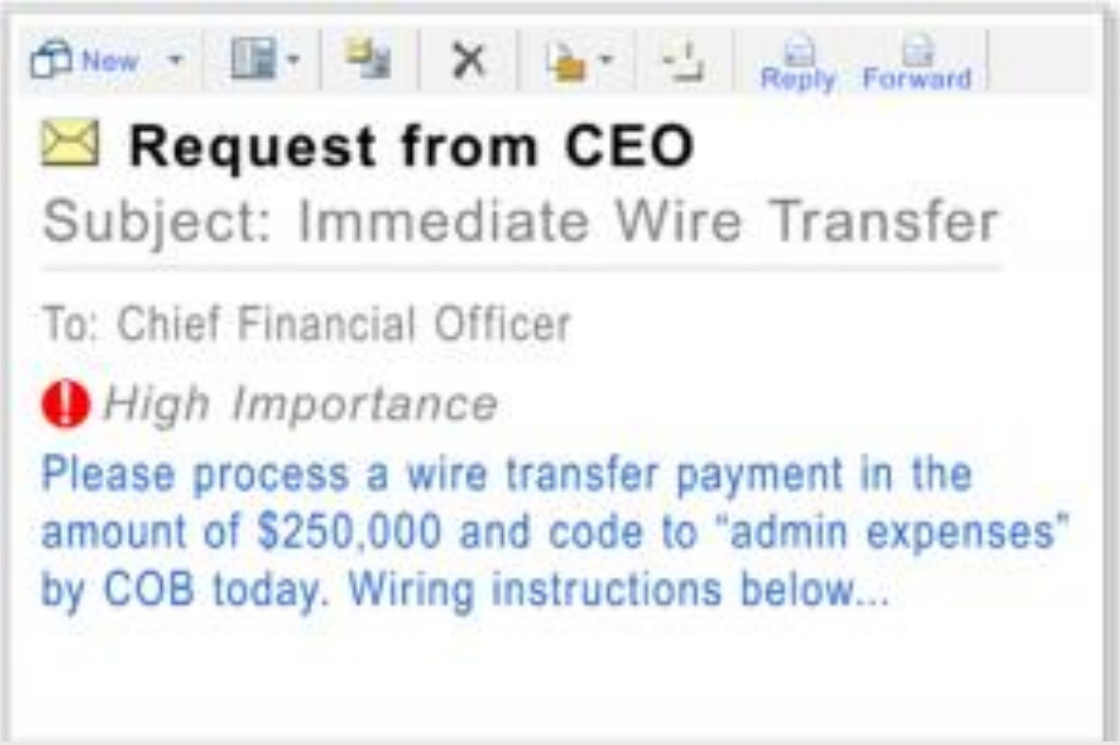
Styles Event Listeners DOM Breakpoints Properties

```
element.style {
}
#banner-hero img {                         global.css:173
   margin:▶0 0 10px;
   position: relative;
   z-index: 1;
}
html, body, div, span, applet,              global.css:17
object, iframe, h1, h2, h3, h4, h5, h6, p,
blockquote, pre, a, abbr, acronym, address,
big, cite, code, del, dfn, em, font, img, ins,
kbd, q, s, samp, small, strike, strong, sub,
sup, tt, var, b, u, i, center, dl, dt, dd, ol,
ul, li, fieldset, form, label, legend, table,
caption, tbody, tfoot, thead, tr, th, td {
   ~~margin:▶0;~~
   padding:▶0;
   border:▶0;
```

▶ background-at…	scroll
▶ background-cl…	border-…
▶ background-co…	rgba(…

Phishing
Wire Transfers

- 270% increase in last 12 months ?
  - No Malware



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

- January 2015, Xoom, $30 million (US)
- Feburary 2015, Scoular, $17.2 million (US)
- August 2015, Ubiquiti Networks, $46.7
- January 2016,FACC, $54 million
- February 2016, Crelan Bank, $76 million

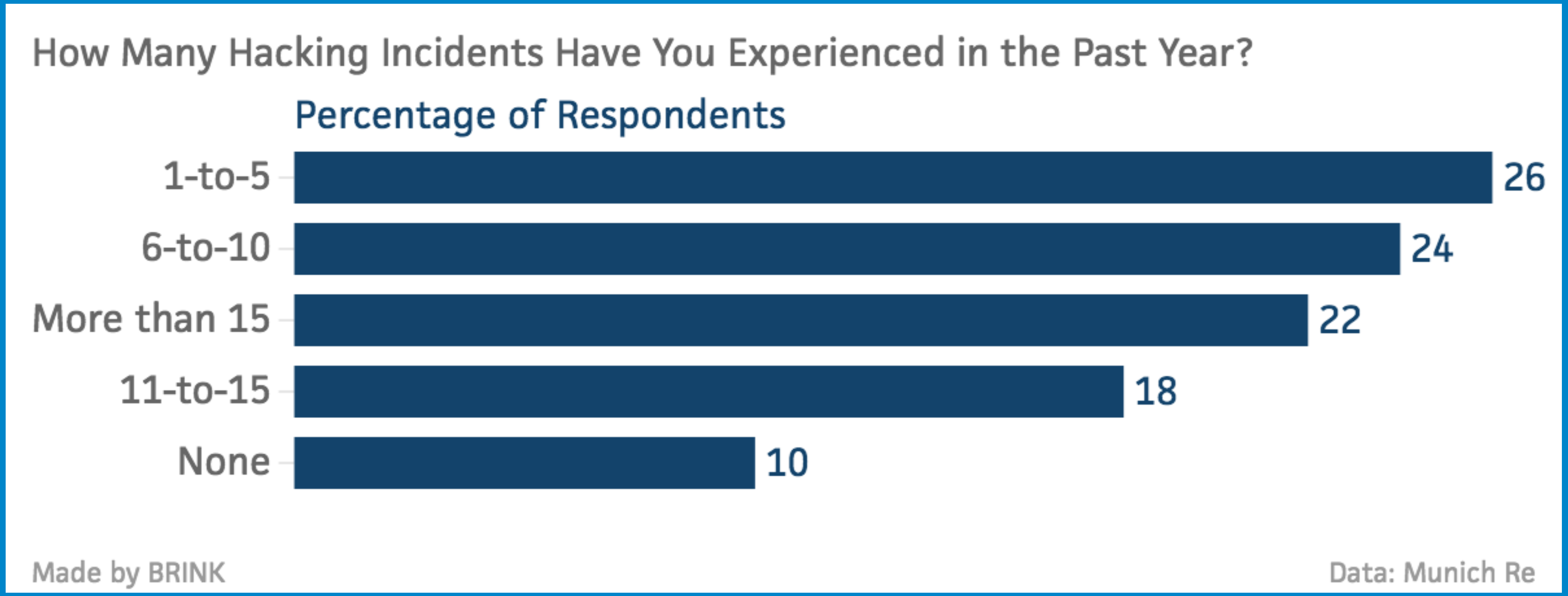
Oct. 2013 to April 4, 2016, the FBI reports losses total a record $2.3 billion, up from $1.2 billion in 2015

SO… EXPECT THE INEVITABLE, AND MOVE ON

Visibility

Response

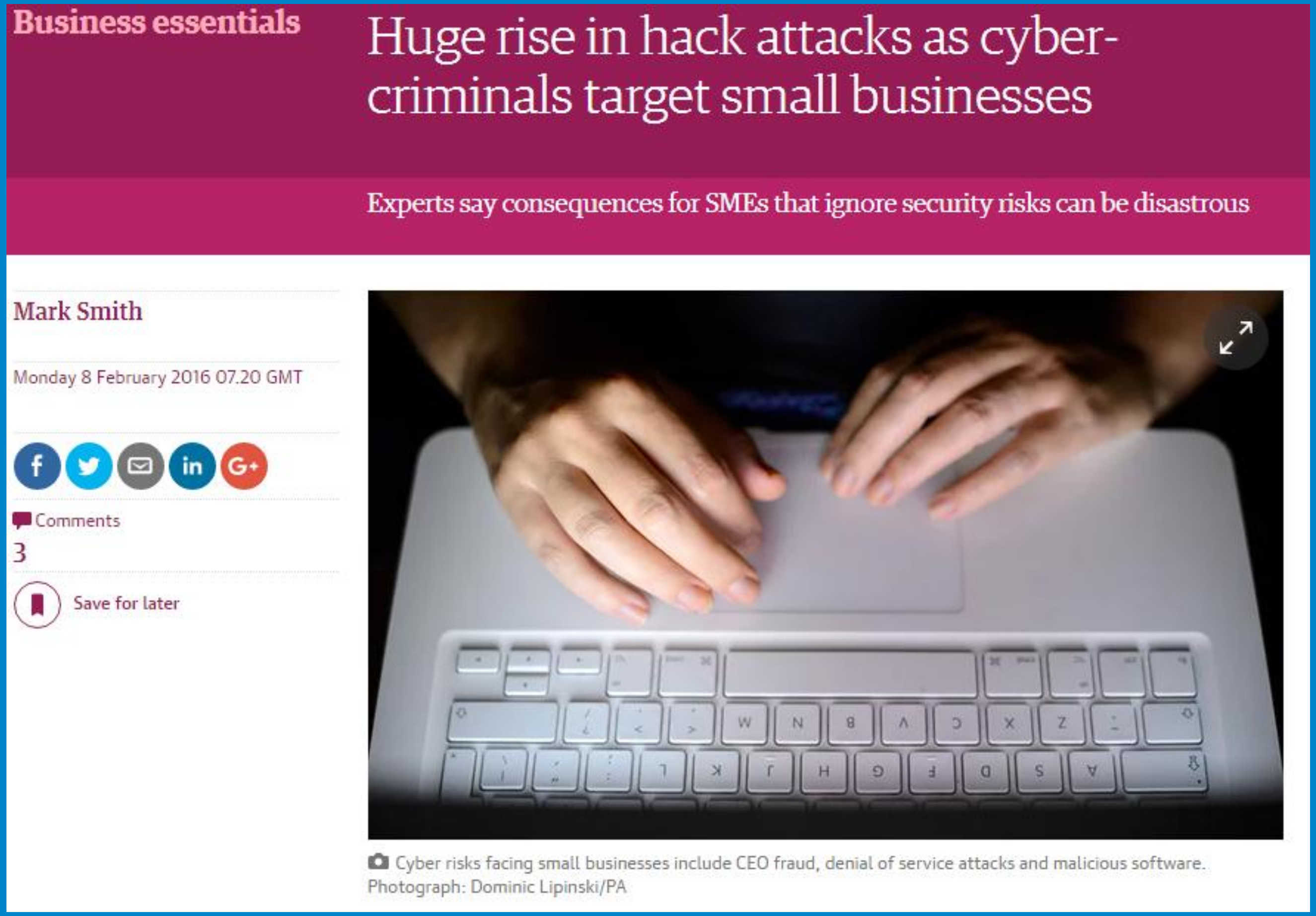
Coverage



How Many Hacking Incidents Have You Experienced in the Past Year?

Made by BRINK

Data: Munich Re



Business essentials

Huge rise in hack attacks as cyber-criminals target small businesses

Experts say consequences for SMEs that ignore security risks can be disastrous

Mark Smith

Monday 8 February 2016 07.20 GMT

Comments 3

Save for later

Cyber risks facing small businesses include CEO fraud, denial of service attacks and malicious software. Photograph: Dominic Lipinski/PA

GDPR

Legal disclaimer

- *All the information shared on proposed EU legislation is subject to change by the European Commission and member states.This is information gathered from the European Commission website and publically available media coverage.*

- *Please do not rely on this information as I am a cyber security practitioner and NOT a legal expert…..otherwise this disclaimer would be longer with many words I would struggle to pronounce correctly….*

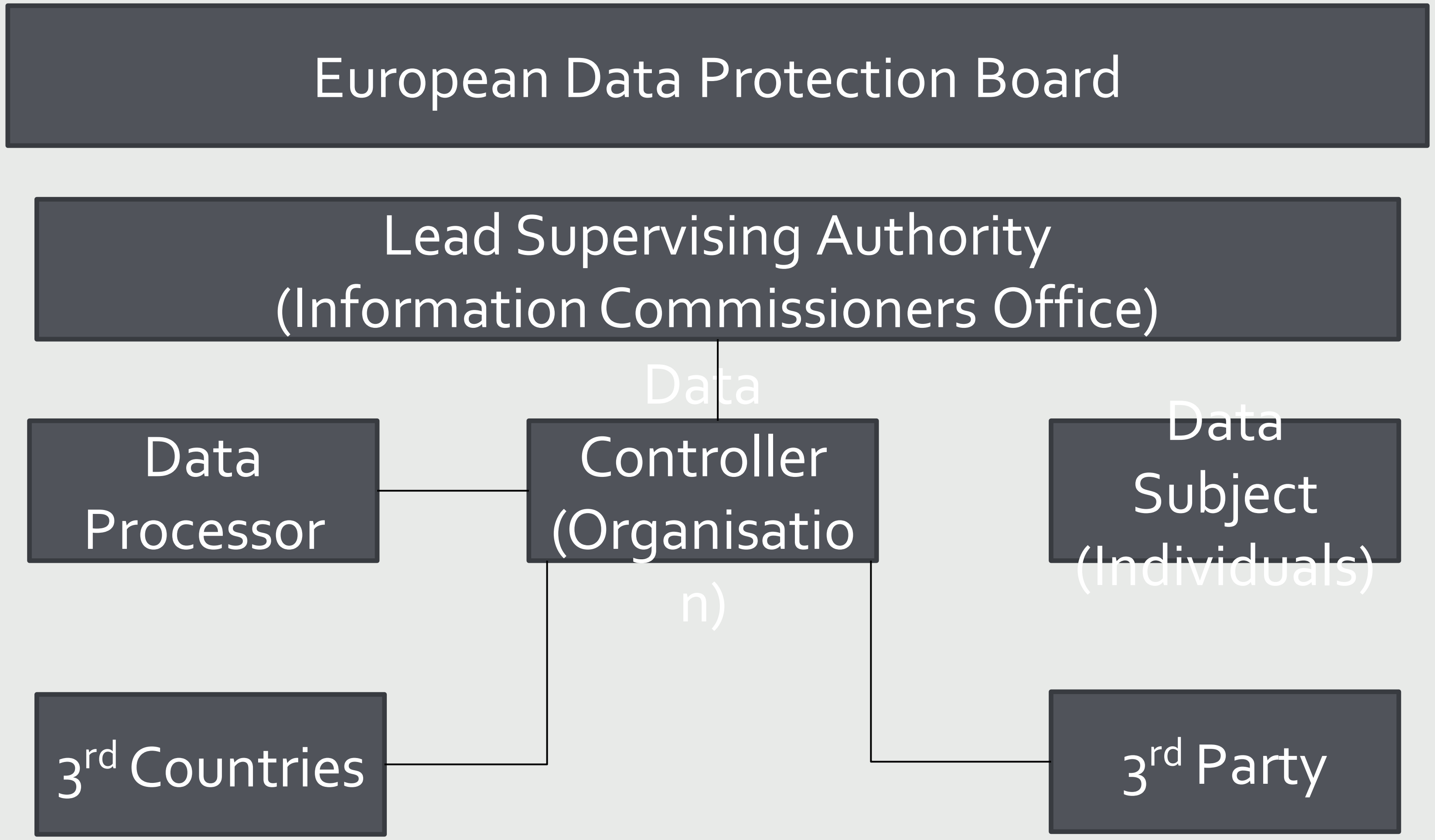
So what is GDPR – Regulation not Directive

- A complete overhaul of data protection regulation with extensive updates of what can be considered identifiable information
- Applies across all member states of the European Union
- Applies to all organisations processing the data of EU data subjects –wherever the organisation is geographically based
- Specific and significant rights for data subjects to seek compensation, rights to erasure and accurate representation
- Fines of up €20,000,00 or 4% global annual turnover
- Significant reduction in that amount based on the implementation of technical, or organisational controls implemented

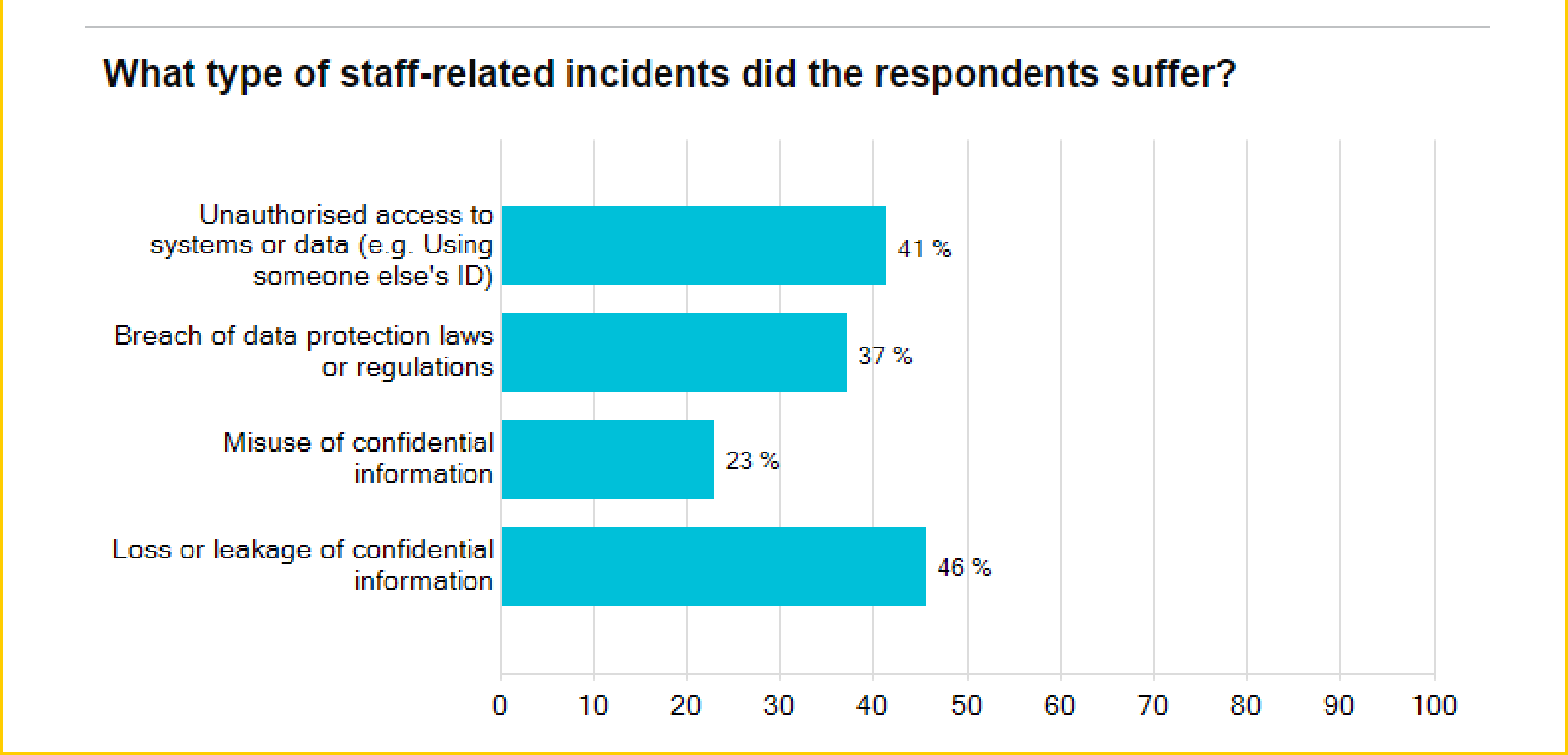
Timing (Brexit)

Midnight 24th May 2018

Structure


European Data Protection Board
Lead Supervising Authority
(Information Commissioners Office)
Data Processor
Data Controller (Organisation)
Data Subject (Individuals)
3rd Countries
3rd Party

https://dm.pwc.com/HMG2015BreachesSurvey/



What type of staff-related incidents did the respondents suffer?

What data is important ?

- Covers all forms of PII vs High risk

- First & last name (combined)
- Home address
- Date/place of birth
- Photos and videos
- Username/password
- National insurance/Social security Number
- Bank account details
- Credit card details
- Passport number
- Medical records
- Financial records
- Personal email addresses/emails
- Biometric data – High risk
- Sexual orientation – High risk

Remedy

Fines are calculated based on several factors:

- Controls already in place
- Nature, gravity, extent and duration of infringement
- The types of personal data involved in the infringement
- Actions taken by the controller or processor to mitigate, negate or notify affected parties (including the ICO) of a breach

Reducing the worry

Visibility

VISIBILITY

- “If you can't measure something, **you can't manage it**”
  Peter Drucker

- Large international investment
  - ‘Outsource everything’
  - Existing solutions, process and toolset

- “My CEO doesn’t believe me”
  - Not been breached
  - Pass the audit

- Difficult to demonstrate before the event that you are protected

LIMITED RESOURCE, SO PRIORITISE WELL

Focus on where damage can be done

Privileged accounts

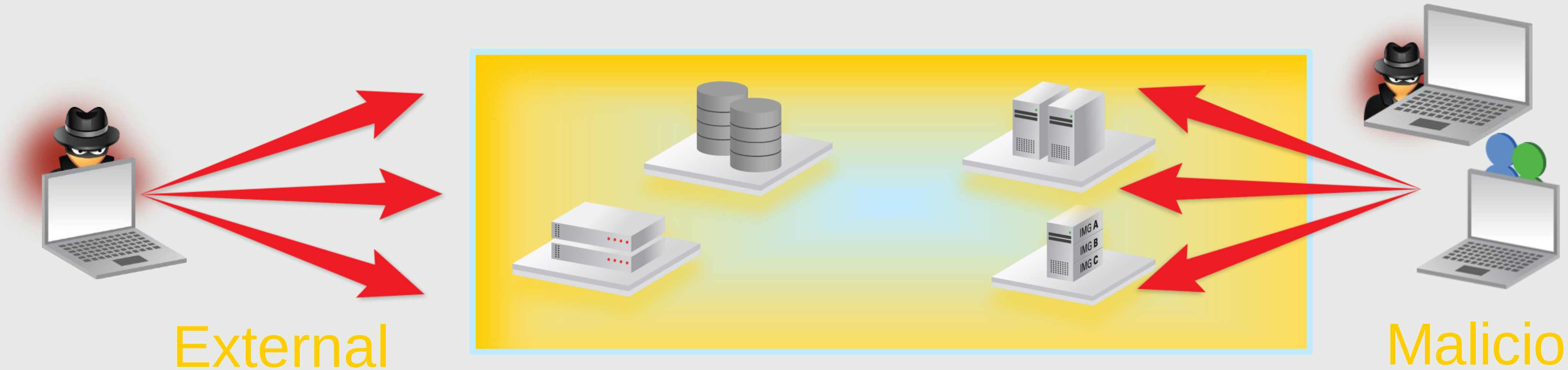
- In-house
- Third-party

DLP

- Location/access/control

In April, a U.S. federal jury ordered Tata Consultancy Services to pay [Epic Systems Corp. $940 million] after a TCS employee used credentials from a previous contract to illegally access confidential data.

THE KEYS TO THE KINGDOM



External Attackers

Malicious Insiders

AN ATTACKER MUST OBTAIN INSIDER CREDENTIALS

"…100% of breaches involved stolen credentials."

"APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts."

Mandiant, M-Trends and APT1 Report

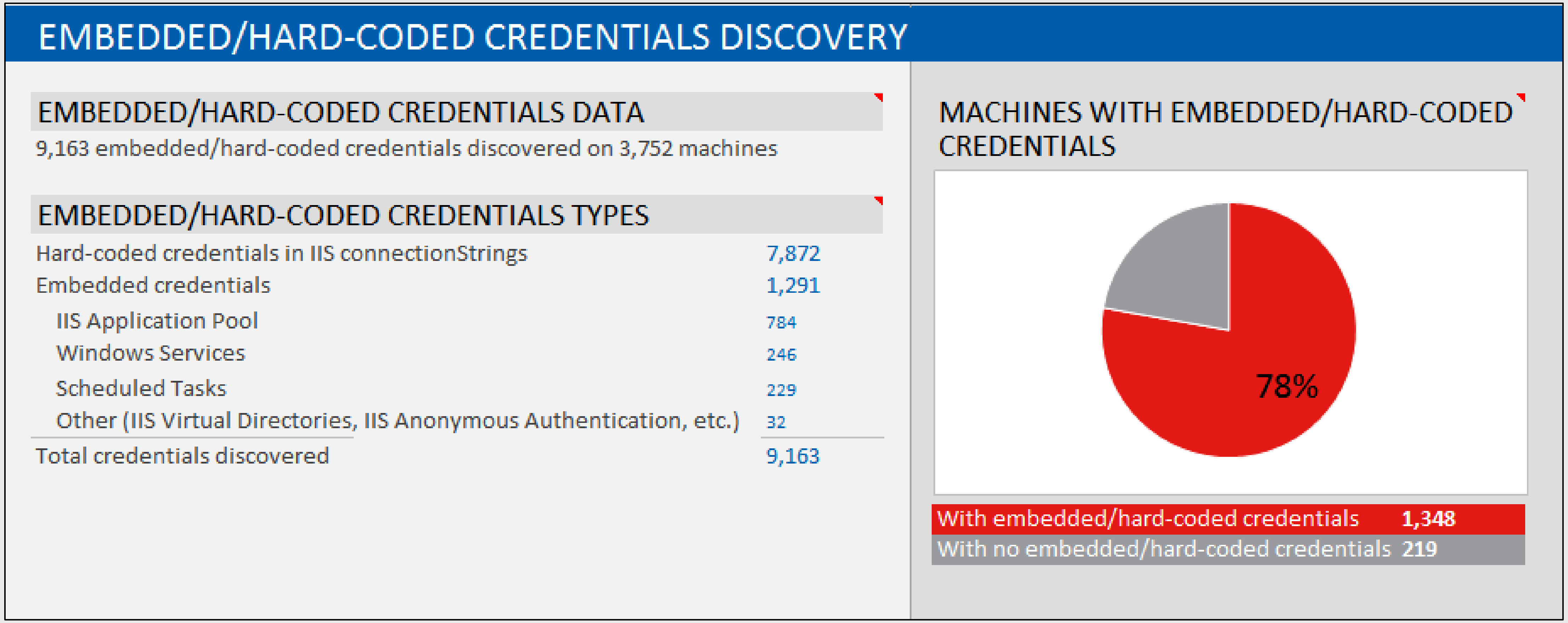
Anything that involves serious intellectual property will be contained in highly secure systems and privileged accounts are the only way hackers can get in." Avivah Litan, VP Distinguished Analyst, 17 years at Gartner , 32 years industry experience

AUDIT AND ANSWER THE QUESTIONS

- On which target servers do privileged accounts exist?
- Which personal admin accounts were created on my servers?
- Which accounts' privileges were escalated?
- Which privileged accounts do not adhere to the company's password policy i.e. password age is greater than 60 days?
- Did one of my contractors add a privileged user to one of the servers?
- Do 'backdoor' application accounts exist on products that have been decommissioned?

Then, and only then, will you know the level of threat and the action/priority that needs to be taken

HARD-CODED CREDENTIALS IN IIS SERVERS



EMBEDDED/HARD-CODED CREDENTIALS DISCOVERY

EMBEDDED/HARD-CODED CREDENTIALS DATA

9,163 embedded/hard-coded credentials discovered on 3,752 machines

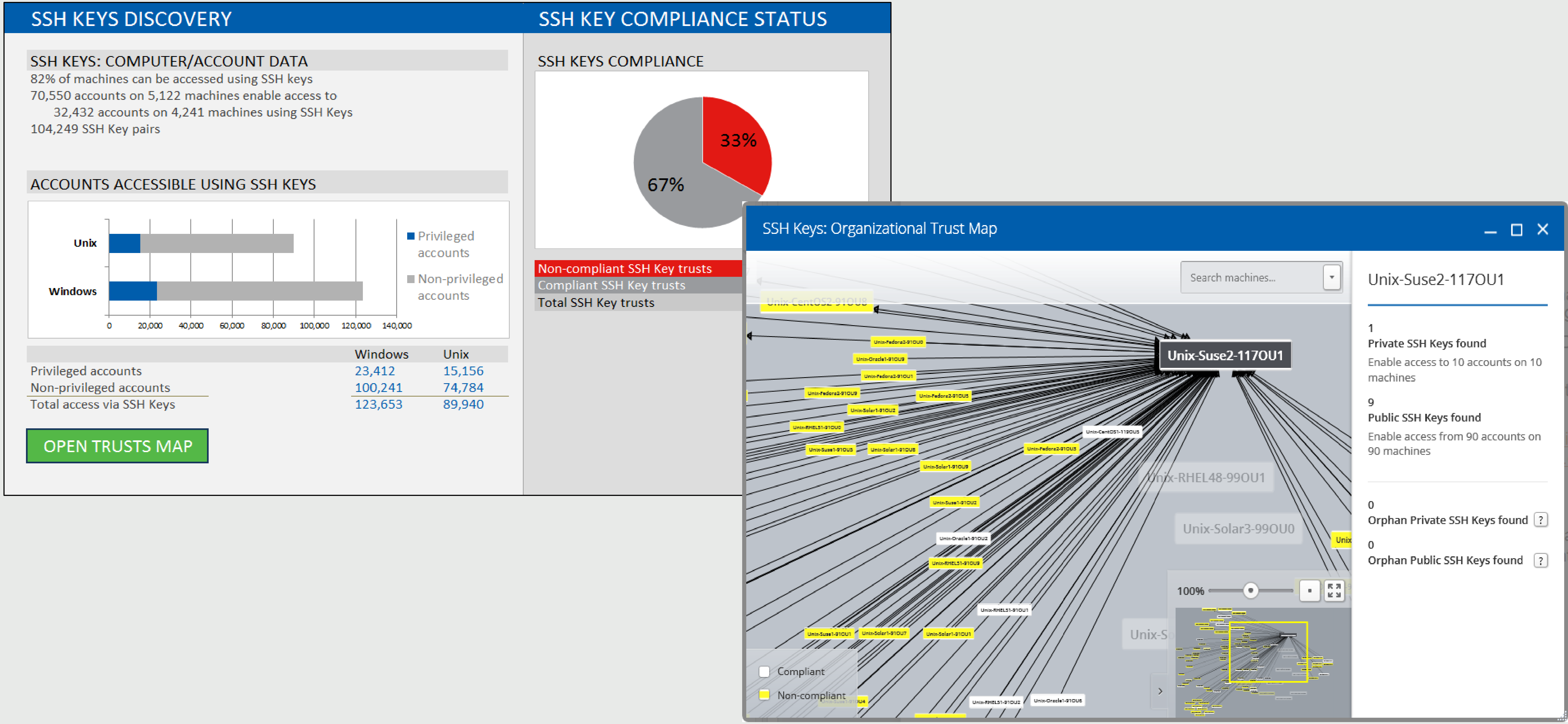
EMBEDDED/HARD-CODED CREDENTIALS TYPES

Hard-coded credentials in IIS connectionStrings	7,872
Embedded credentials	1,291
IIS Application Pool	784
Windows Services	246
Scheduled Tasks	229
Other (IIS Virtual Directories, IIS Anonymous Authentication, etc.)	32
Total credentials discovered	9,163

MACHINES WITH EMBEDDED/HARD-CODED CREDENTIALS

With embedded/hard-coded credentials	1,348
With no embedded/hard-coded credentials	219

SSH KEY DISCOVERY RESULTS



SSH KEYS DISCOVERY

SSH KEYS: COMPUTER/ACCOUNT DATA

82% of machines can be accessed using SSH keys

70,550 accounts on 5,122 machines enable access to

32,432 accounts on 4,241 machines using SSH Keys

104,249 SSH Key pairs

ACCOUNTS ACCESSIBLE USING SSH KEYS

	Windows	Unix
Privileged accounts	23,412	15,156
Non-privileged accounts	100,241	74,784
Total access via SSH Keys	123,653	89,940

OPEN TRUSTS MAP

SSH KEY COMPLIANCE STATUS

SSH KEYS COMPLIANCE

Non-compliant SSH Key trusts

Compliant SSH Key trusts

Total SSH Key trusts

SSH Keys: Organizational Trust Map

□ Compliant

🟨 Non-compliant

Unix-Suse2-117OU1

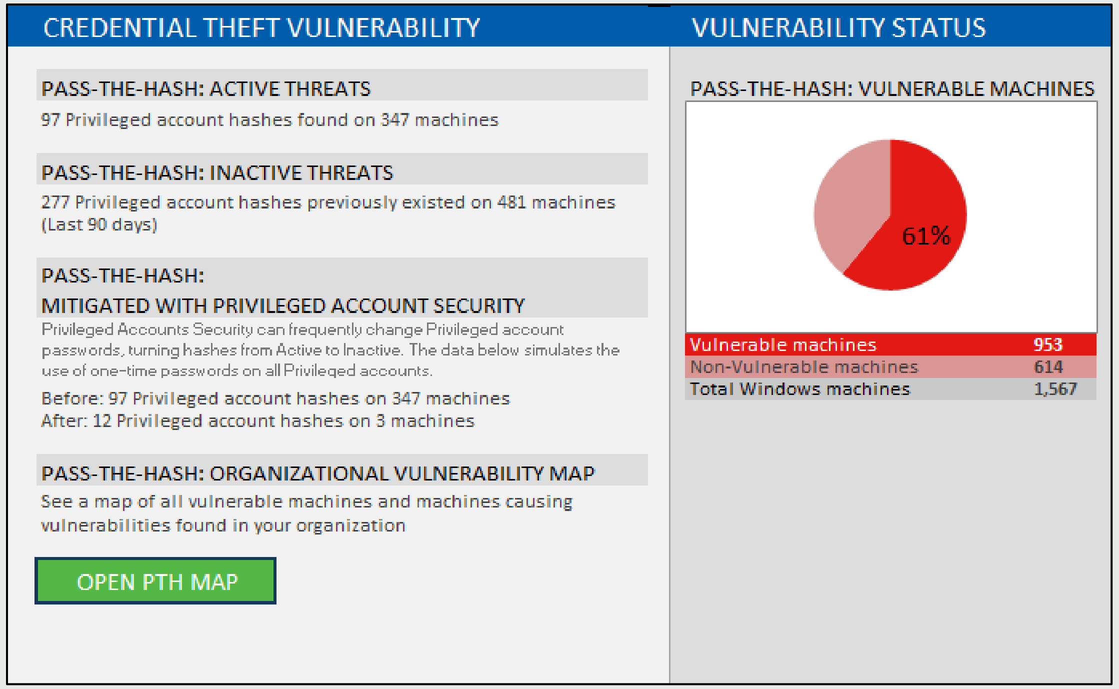
1
Private SSH Keys found
Enable access to 10 accounts on 10 machines

9
Public SSH Keys found
Enable access from 90 accounts on 90 machines

0
Orphan Private SSH Keys found ?

0
Orphan Public SSH Keys found ?

PASS-THE-HASH VULNERABILITIES RESULTS



CREDENTIAL THEFT VULNERABILITY

PASS-THE-HASH: ACTIVE THREATS

97 Privileged account hashes found on 347 machines

PASS-THE-HASH: INACTIVE THREATS

277 Privileged account hashes previously existed on 481 machines (Last 90 days)

PASS-THE-HASH: MITIGATED WITH PRIVILEGED ACCOUNT SECURITY

Privileged Accounts Security can frequently change Privileged account passwords, turning hashes from Active to Inactive. The data below simulates the use of one-time passwords on all Privileged accounts.

Before: 97 Privileged account hashes on 347 machines
After: 12 Privileged account hashes on 3 machines

PASS-THE-HASH: ORGANIZATIONAL VULNERABILITY MAP

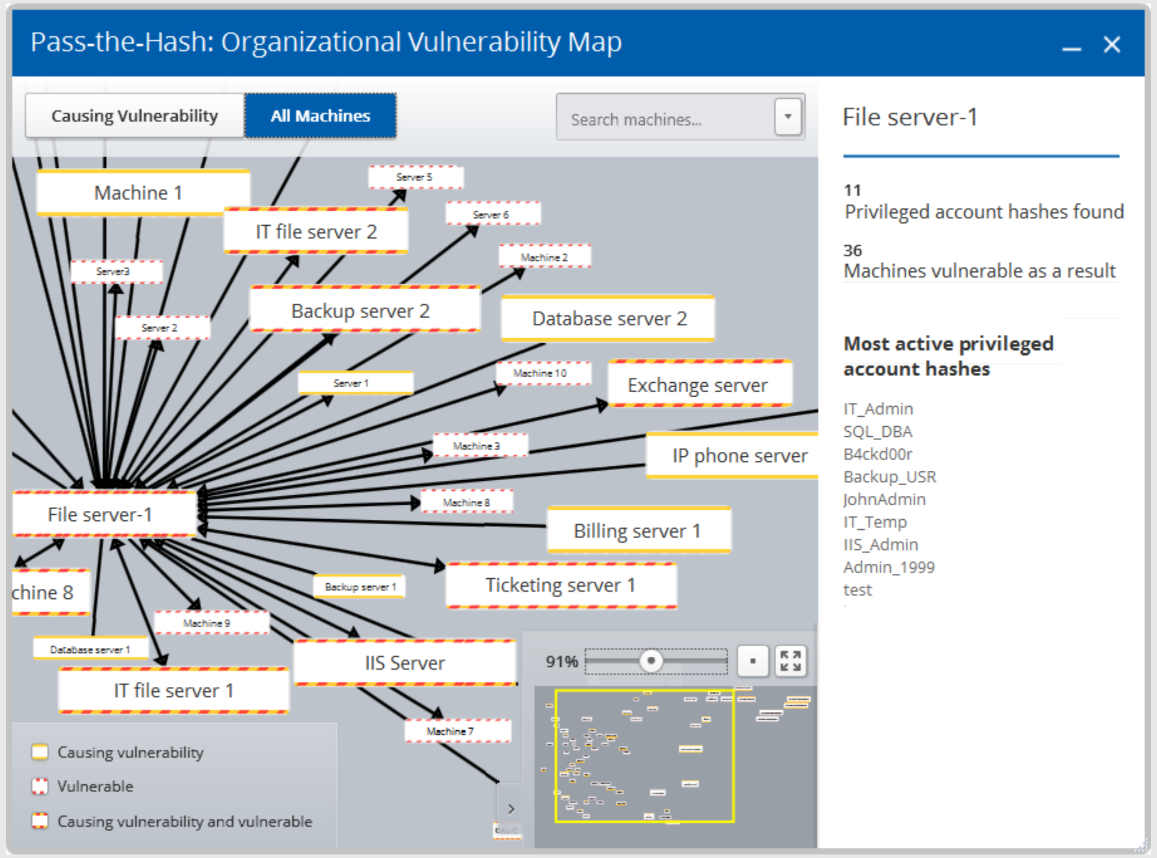
See a map of all vulnerable machines and machines causing vulnerabilities found in your organization

OPEN PTH MAP

VULNERABILITY STATUS

PASS-THE-HASH: VULNERABLE MACHINES

Vulnerable machines	953
Non-Vulnerable machines	614
Total Windows machines	1,567



Pass-the-Hash: Organizational Vulnerability Map

File server-1

11
Privileged account hashes found

36
Machines vulnerable as a result

Most active privileged account hashes

IT_Admin
SQL_DBA
B4ckd00r
Backup_USR
JohnAdmin
IT_Temp
IIS_Admin
Admin_1999
test

Fear or fact

DATA LOSS (USER CREATED DOCS)
IS THERE AN ISSUE?

Figure 1. Is there company data you have access to that you probably should not see?

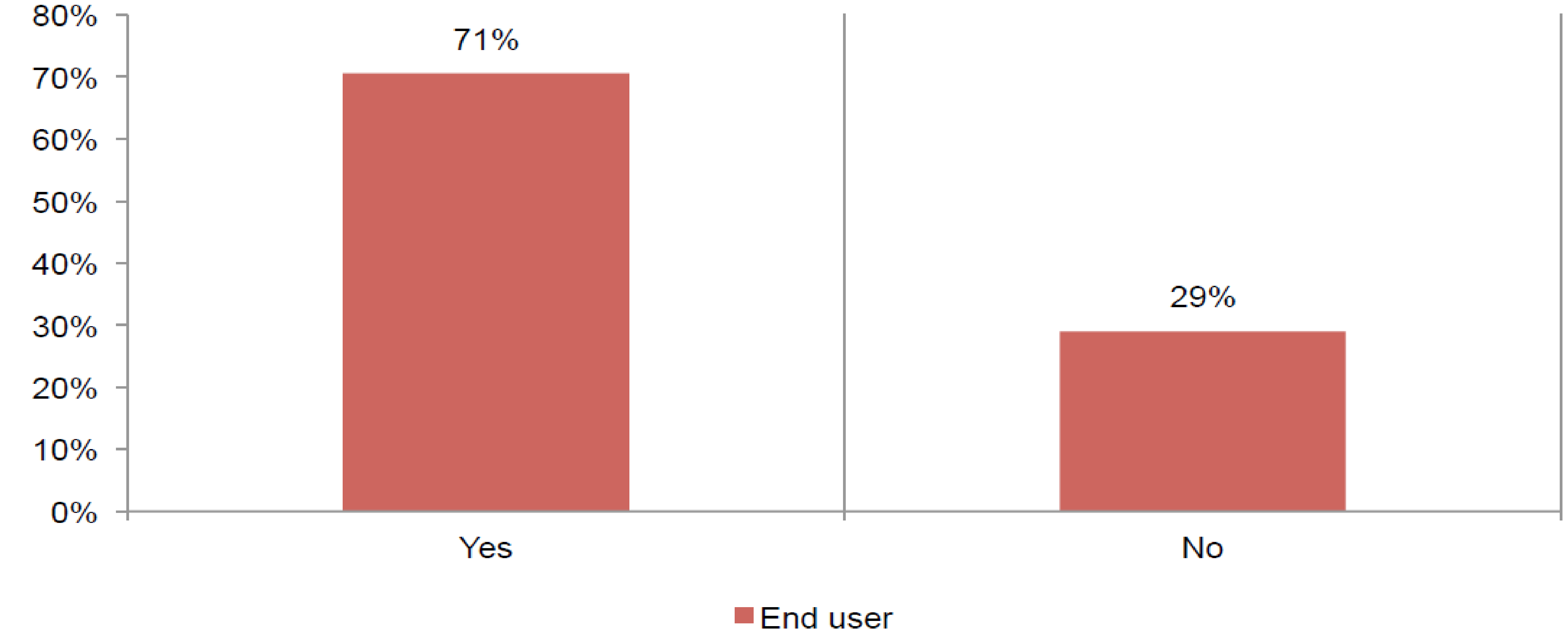


Figure 4. Does your organization enforce a strict least privilege model?

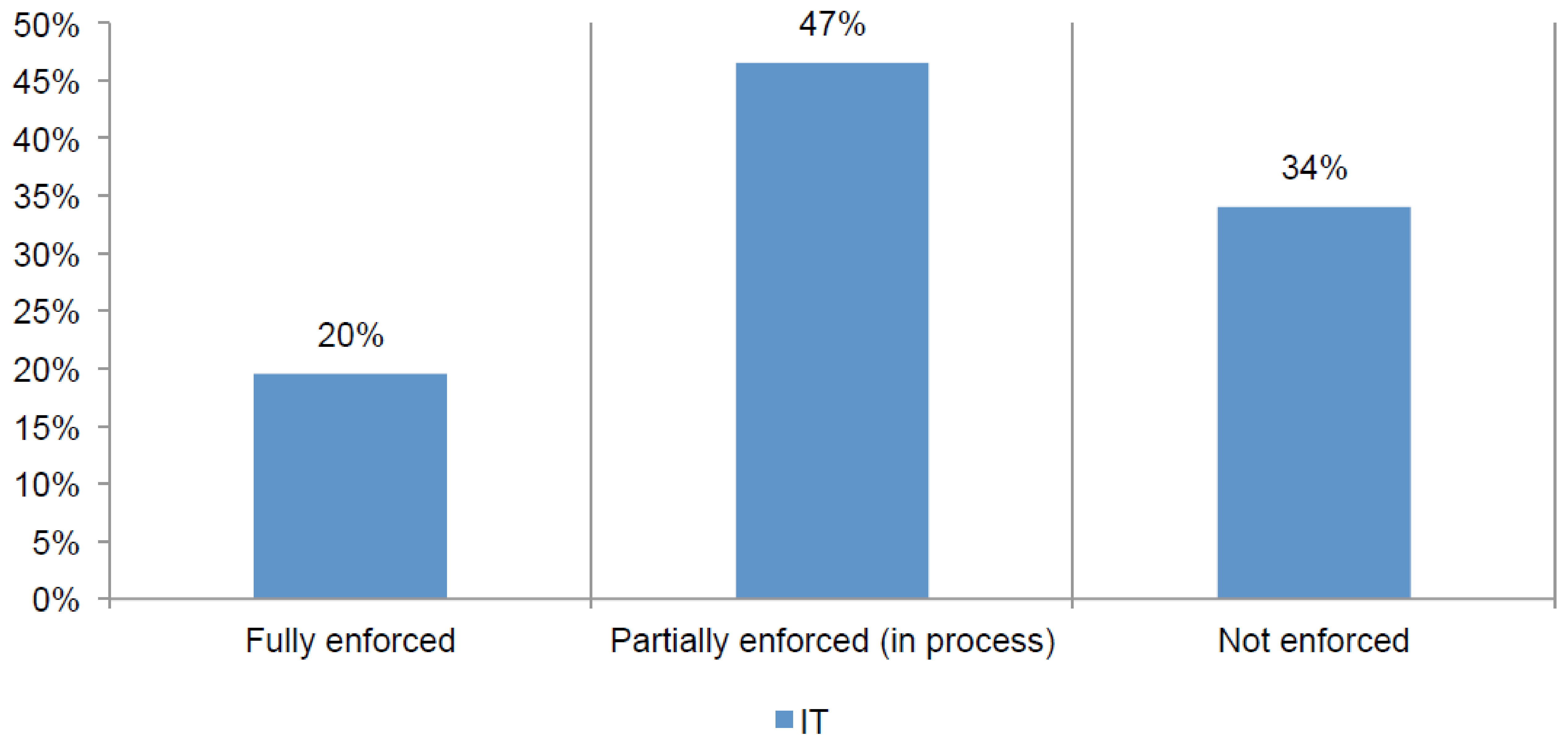
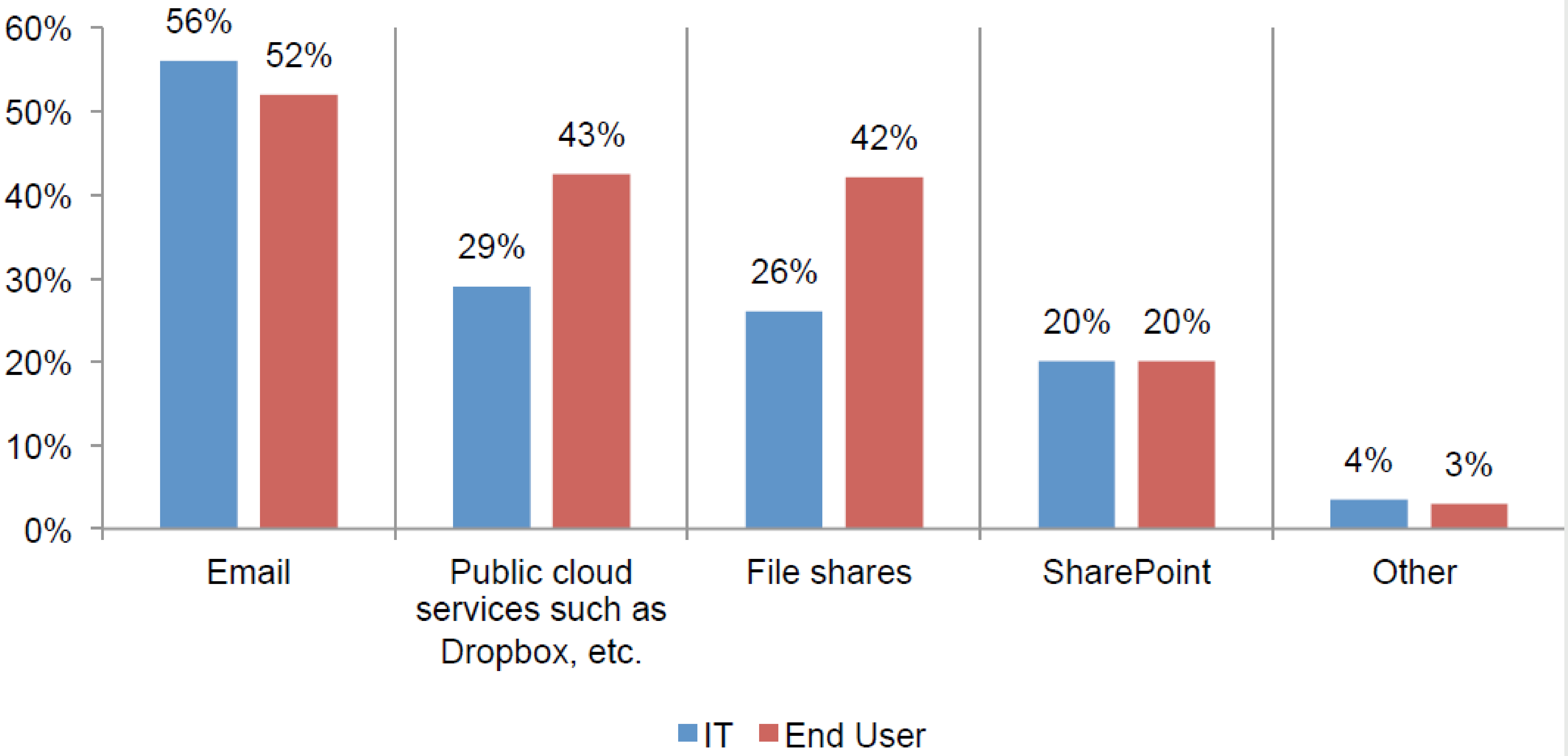


Figure 12. The preferred ways to share company data or files with co-workers
Two responses permitted



ROOT OF THE PROBLEM

There are many questions IT and the business can't answer:

Who has access to files, folders, mailboxes?

Who is accessing, modifying, moving, deleting files and email?

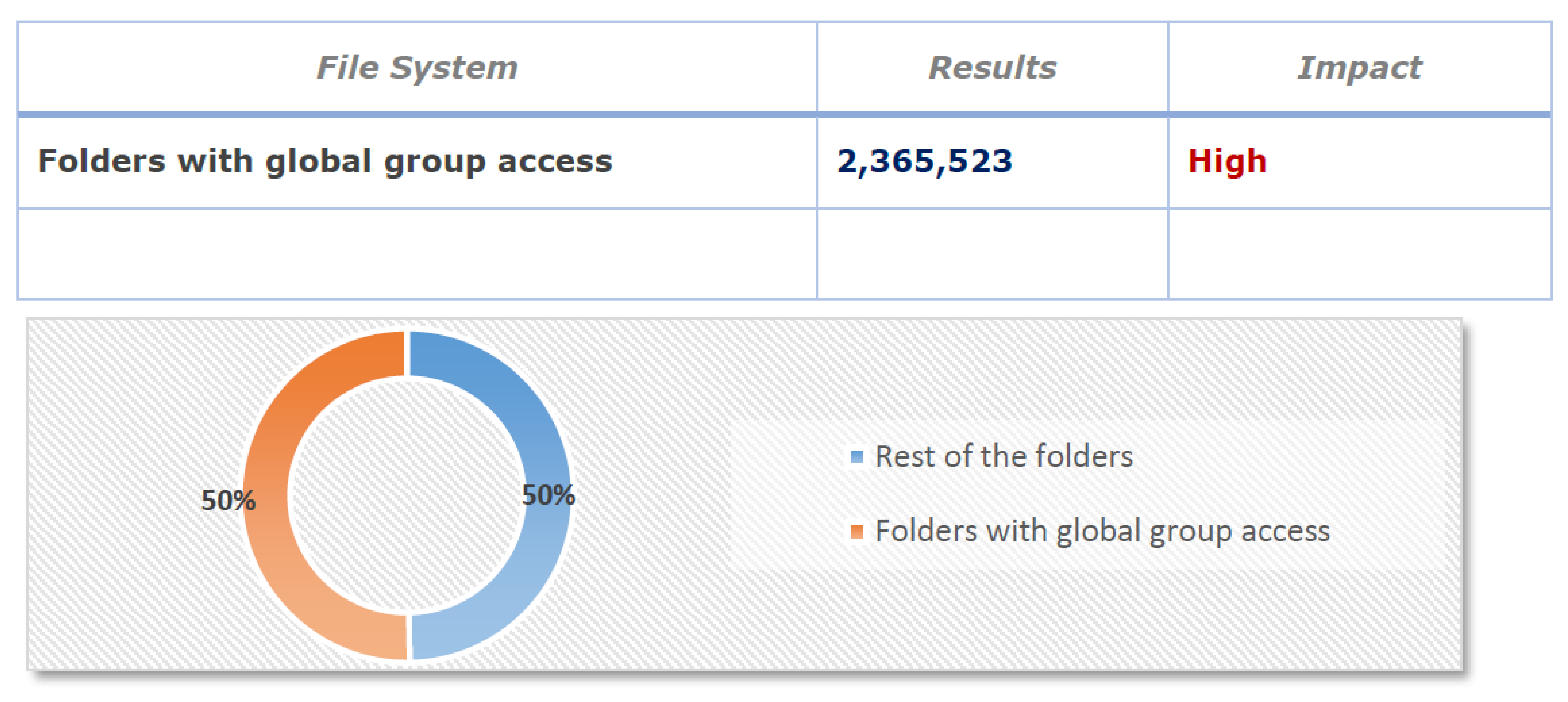
Which files contain critical information?

Which data is exposed to too many people?

Who owns data?

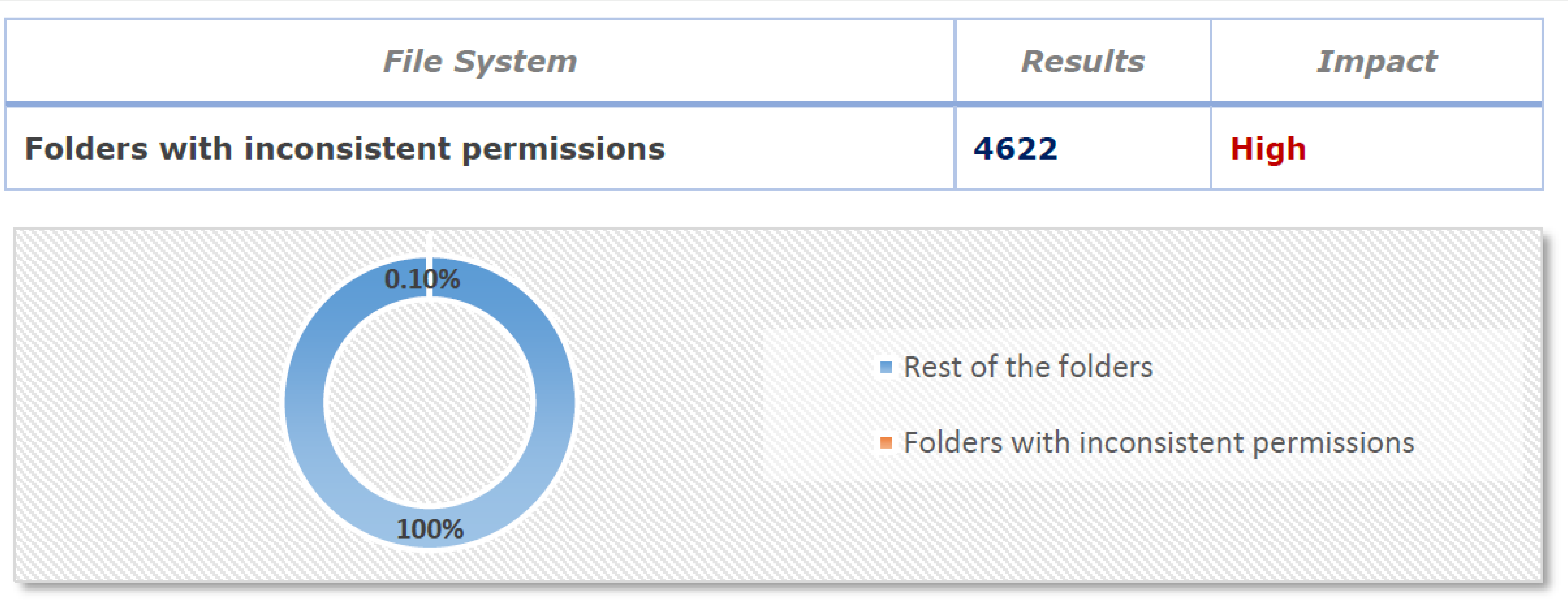
What data isn't being used?

FOLDERS WITH GLOBAL GROUP ACCESS



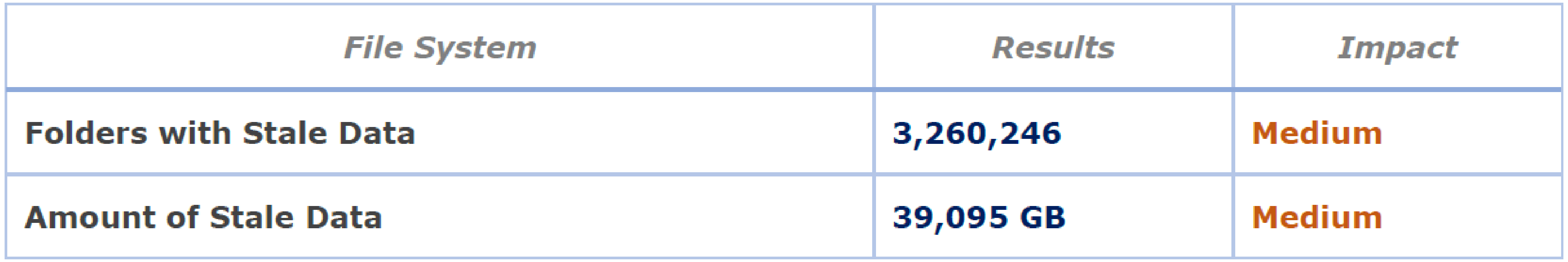
File System	*Results*	*Impact*
Folders with global group access	**2,365,523**	**High**

FOLDERS WITH INCONSISTENT PERMISSIONS

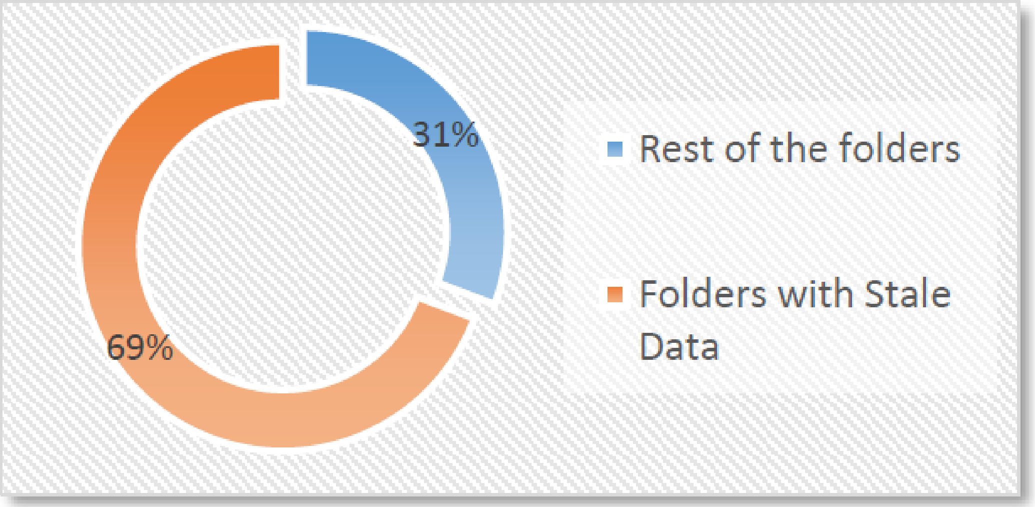


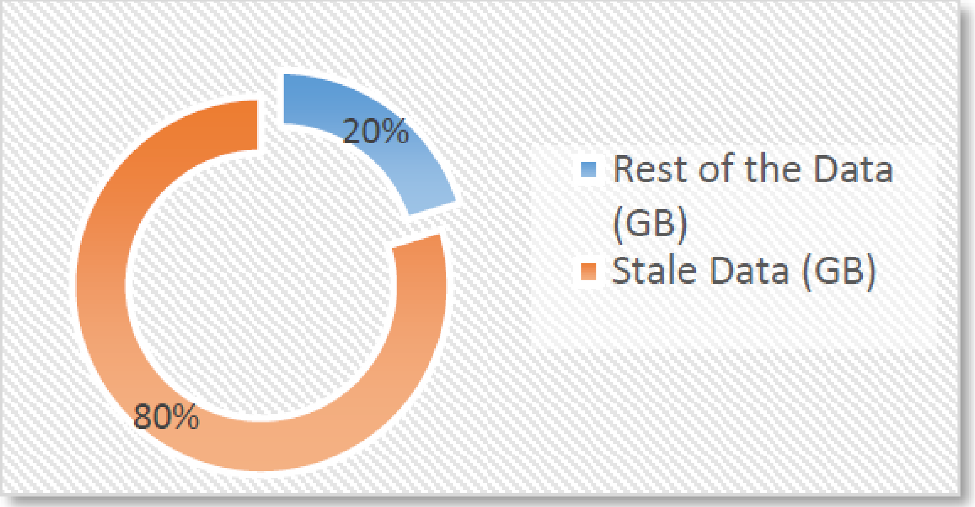
File System	*Results*	*Impact*
Folders with inconsistent permissions	**4622**	**High**

FOLDERS WITH STALE DATA
AMOUNT OF STALE DATA



File System	*Results*	*Impact*
Folders with Stale Data	**3,260,246**	**Medium**
Amount of Stale Data	**39,095 GB**	**Medium**





SUMMARY OF VISIBILITY REPORTS AND ASSESSMENTS

- Visibility reports are generally ‘free’
  - IT resource
  - Management time
  - Consultancy time

- You know the business best
  - State of the nation
  - Scale of challenge

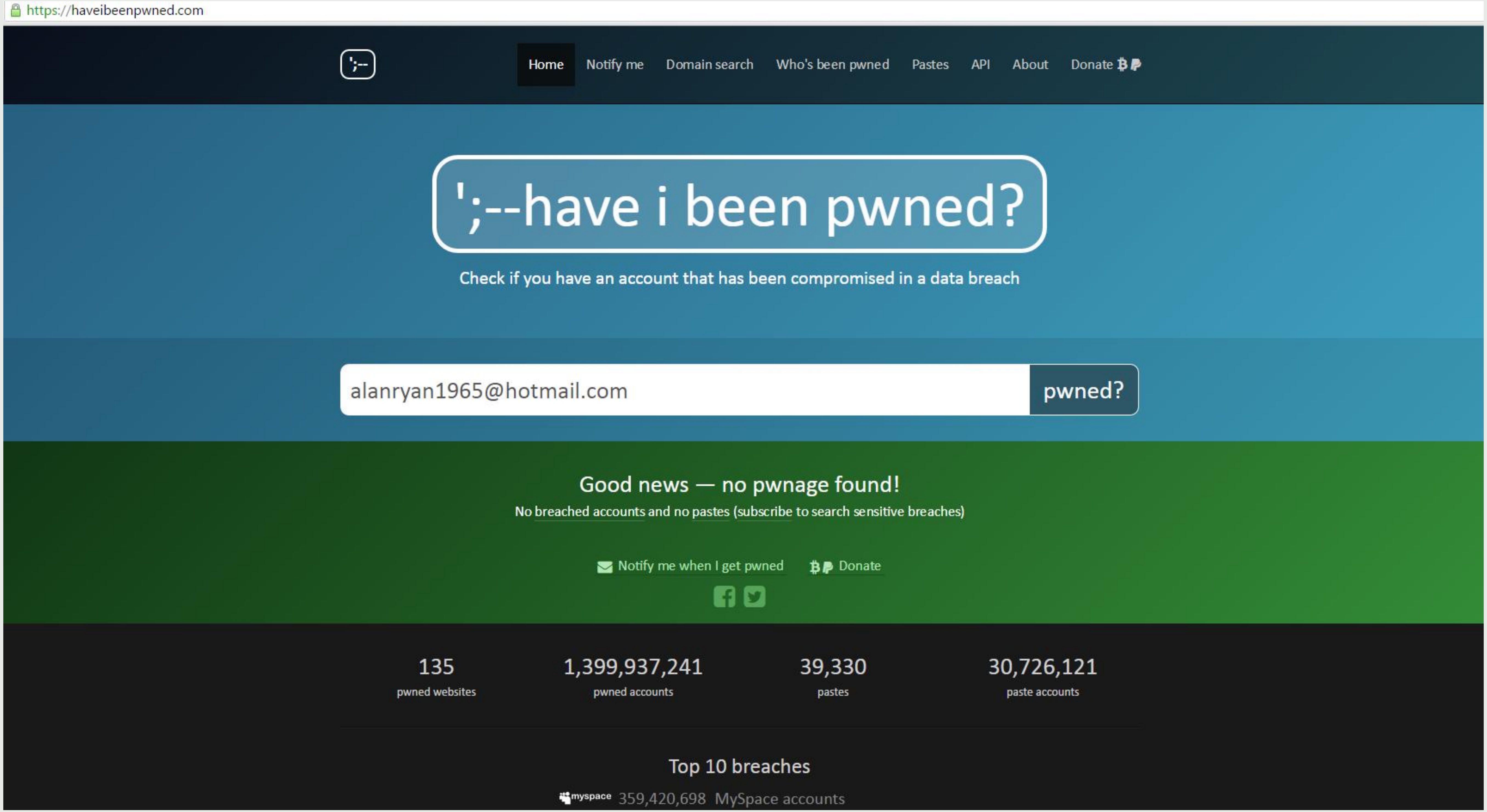
- Allows prioritisation

TESTING THE SYSTEMS AND PROCESSES

- Penetration testing is only a part of the solution
- Look at processes
  - Leavers, joiners, movers
- Social engineering
- Governance is more easily achieved when automated

Social engineering

- Waterering Hole attacks – facebook
- Out of office
- Boss – pubs and bars, surveillance



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

alanryan1965@hotmail.com

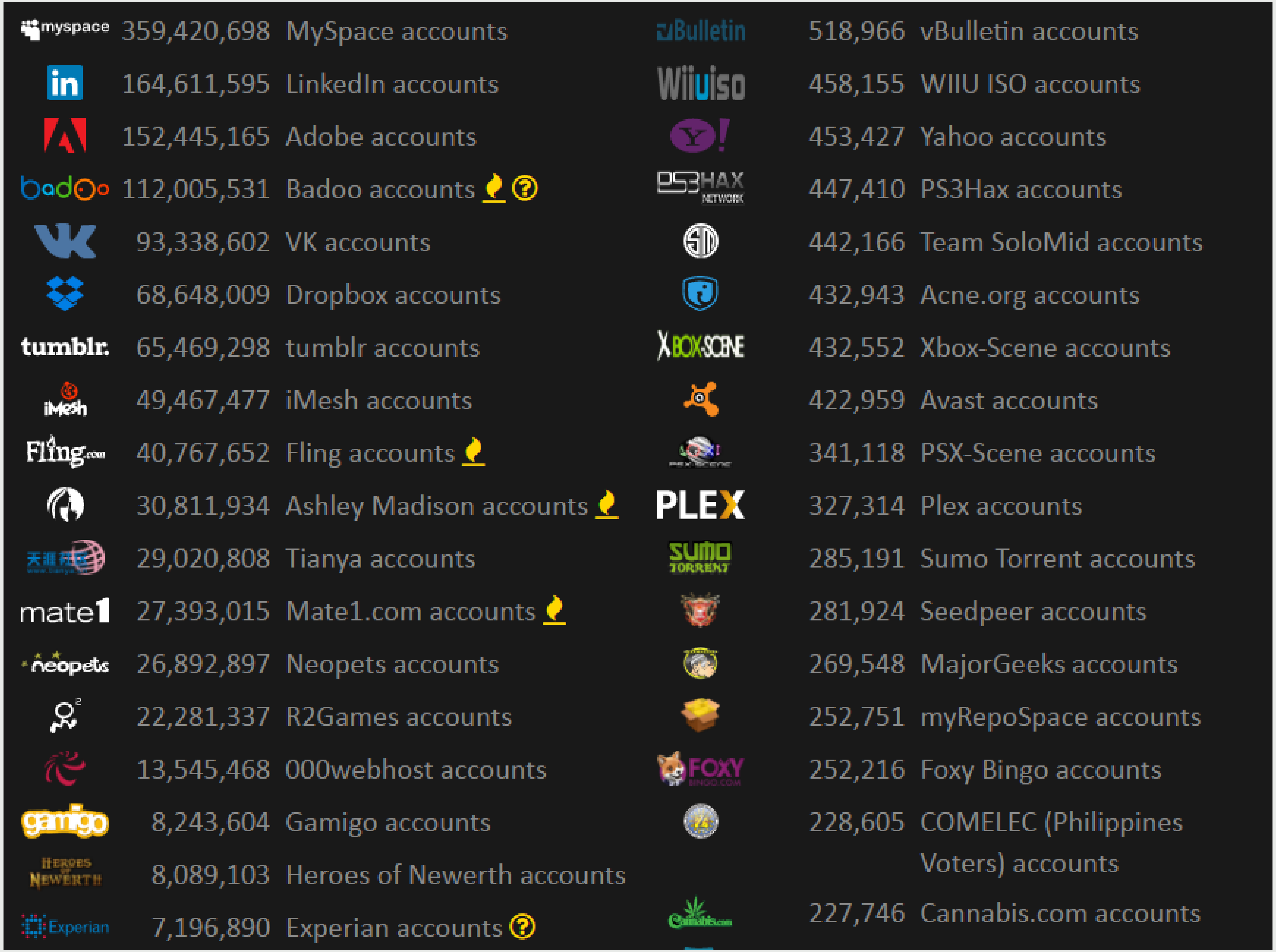
Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

135	1,399,937,241	39,330	30,726,121
pwned websites	pwned accounts	pastes	paste accounts

Top 10 breaches

myspace 359,420,698 MySpace accounts



359,420,698	MySpace accounts	518,966	vBulletin accounts
164,611,595	LinkedIn accounts	458,155	WIIU ISO accounts
152,445,165	Adobe accounts	453,427	Yahoo accounts
112,005,531	Badoo accounts 🔥 ?	447,410	PS3Hax accounts
93,338,602	VK accounts	442,166	Team SoloMid accounts
68,648,009	Dropbox accounts	432,943	Acne.org accounts
65,469,298	tumblr accounts	432,552	Xbox-Scene accounts
49,467,477	iMesh accounts	422,959	Avast accounts
40,767,652	Fling accounts 🔥	341,118	PSX-Scene accounts
30,811,934	Ashley Madison accounts 🔥	327,314	Plex accounts
29,020,808	Tianya accounts	285,191	Sumo Torrent accounts
27,393,015	Mate1.com accounts 🔥	281,924	Seedpeer accounts
26,892,897	Neopets accounts	269,548	MajorGeeks accounts
22,281,337	R2Games accounts	252,751	myRepoSpace accounts
13,545,468	000webhost accounts	252,216	Foxy Bingo accounts
8,243,604	Gamigo accounts	228,605	COMELEC (Philippines Voters) accounts
8,089,103	Heroes of Newerth accounts	227,746	Cannabis.com accounts
7,196,890	Experian accounts ?		

Why should I care about “Linked-in”

- Common passwords
- Webmail
- Malware

SUMMARY

- Breaches are inevitable

- Resources and budgets are limited where as IT continues to grow
- Insider threats are most common and yet we spend too much on outsider threats

- Privileged accounts are a key area where a real impact can be made

- There are solutions available but Visibility is the first step as only then can you Prioritise

- Use a services company to test the processes, various schemes

- With GDPR, you have a much higher level of responsibility and given we have stated the inevitable will happen, you need to show you have mitigated.