Security & Ethics – Aug 2015

UKZN
MBA
2015

Justin Williams
Director
ITSec.org.za

A Thought….

- *“Computer insecurity is inevitable. Networks will be hacked. Fraud will be committed. Money will be lost. People will die”.*
- *Bruce Schneier, master cryptographer*

A Thought….

PERSONNEL
I SEE YOU'VE DONE HARD TIME FOR COMPUTER HACKING... WHEN CAN YOU START?

Ethics

- IT has the potential to do good vs potential for harm
- Principles of Technology Ethics
  - Proportionality – good outweigh harm
  - Informed Consent – those affected understand and accept
  - Justice – benefits and burdens should be fairly distributed
  - Minimized risk – even if acceptable by other 3 guidelines, must be implemented to avoid risk

Ethics

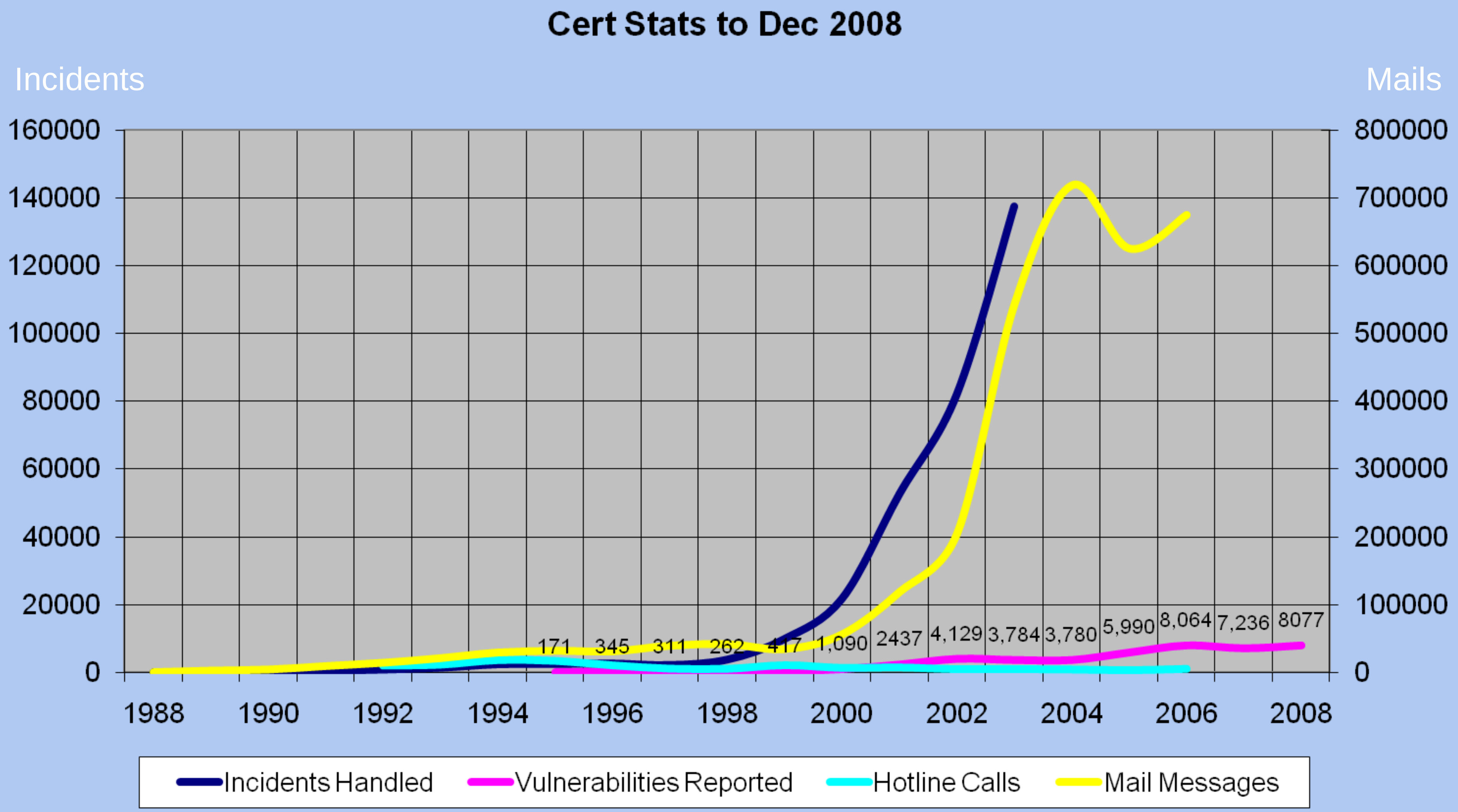
- Ethics are embodied in codes of professional conduct for IS professionals
  - Eg. Association of IT professionals (AITP), ISACA, ISC2
    - HTTP://WWW.ISACA.ORG.ZA
  - Recognises obligation to employer
    - Avoid conflicts of interest
    - Protect privacy & confidentiality etc
  - Also obligation to society
    - Ensure products of work used responsibly
    - Support, respect and abide by laws
    - Never use confidential info for personal gain

Security Question for the day

- How did Osama Bin Laden outsmart the US (and the world's) intelligence agencies for so long?

- Answer later

Growth in number of security breaches



Cert Stats to Dec 2008

Insights on
governance, risk
and compliance

October 2013

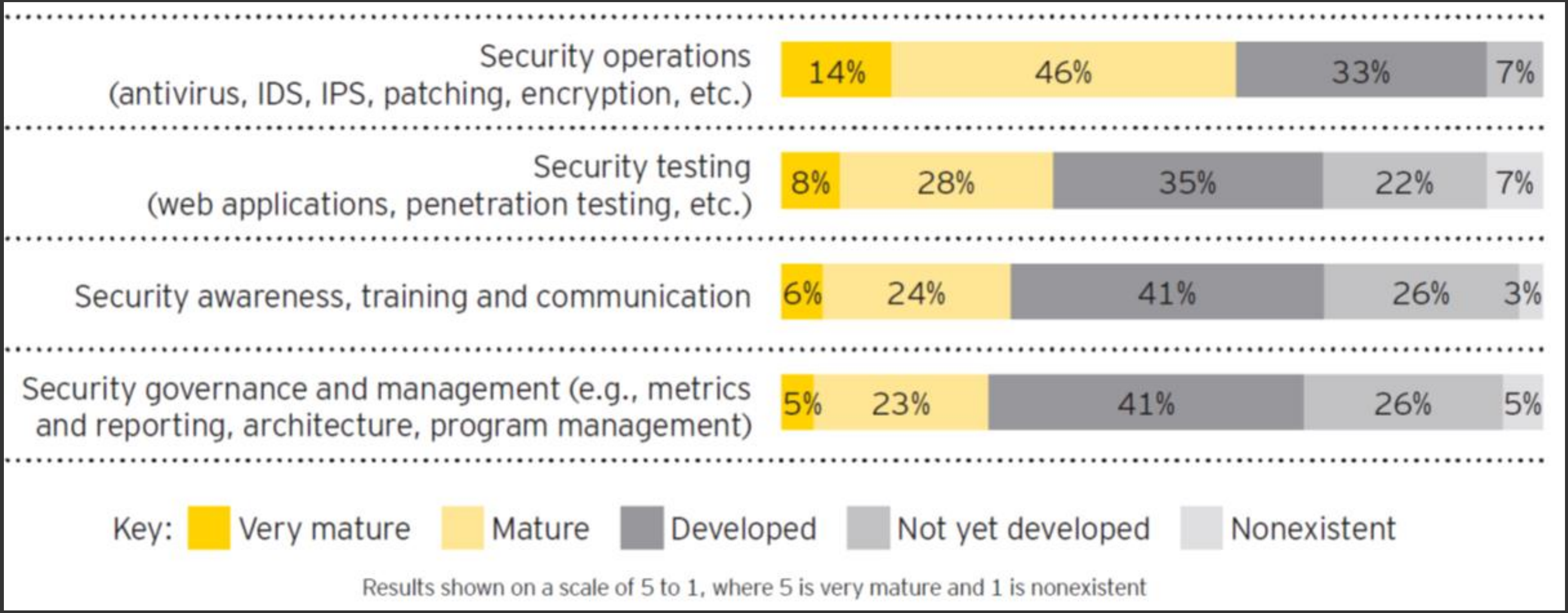
Under cyber attack

EY's Global Information Security Survey 2013

EY

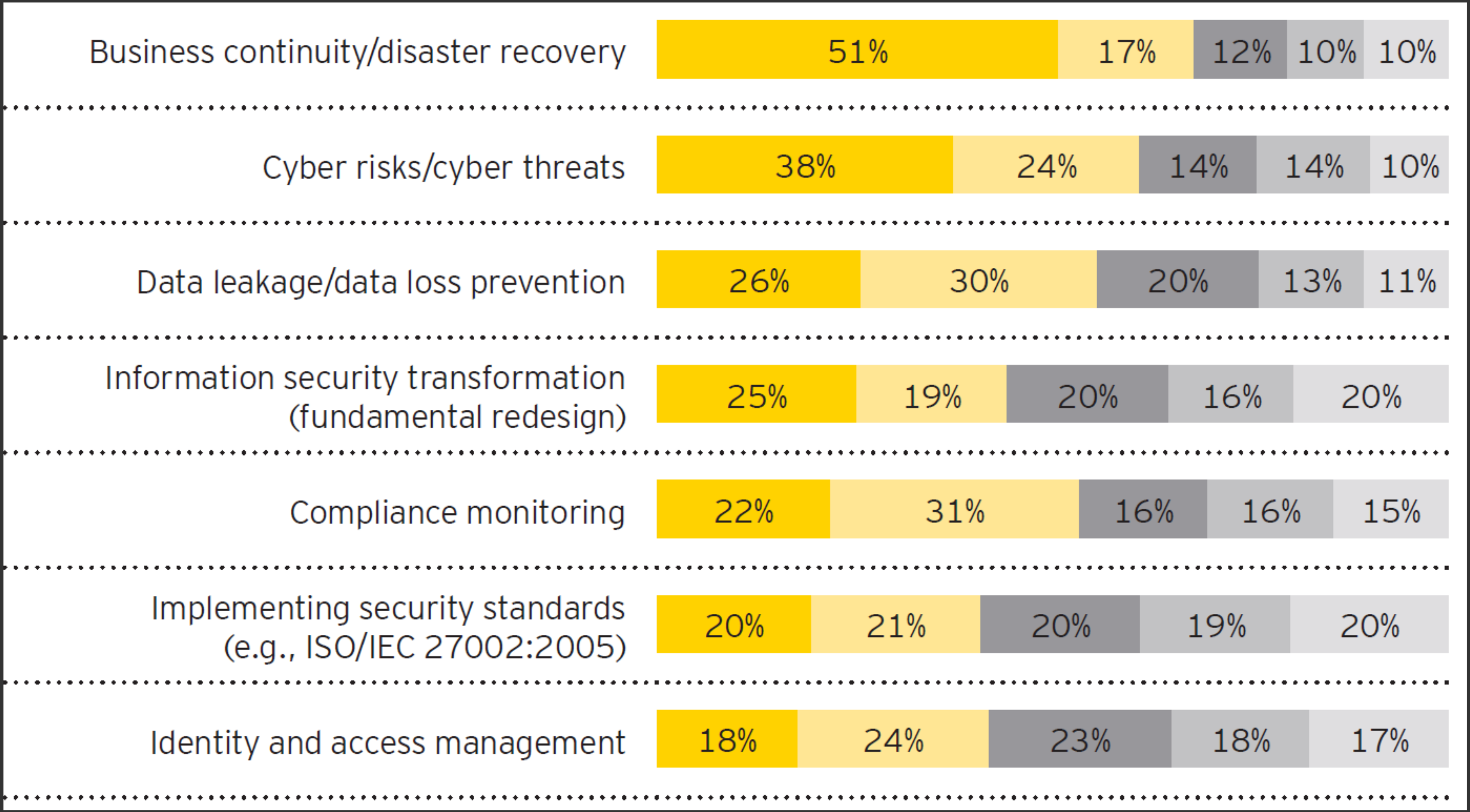
Building a better
working world

Maturity of infosec management processes



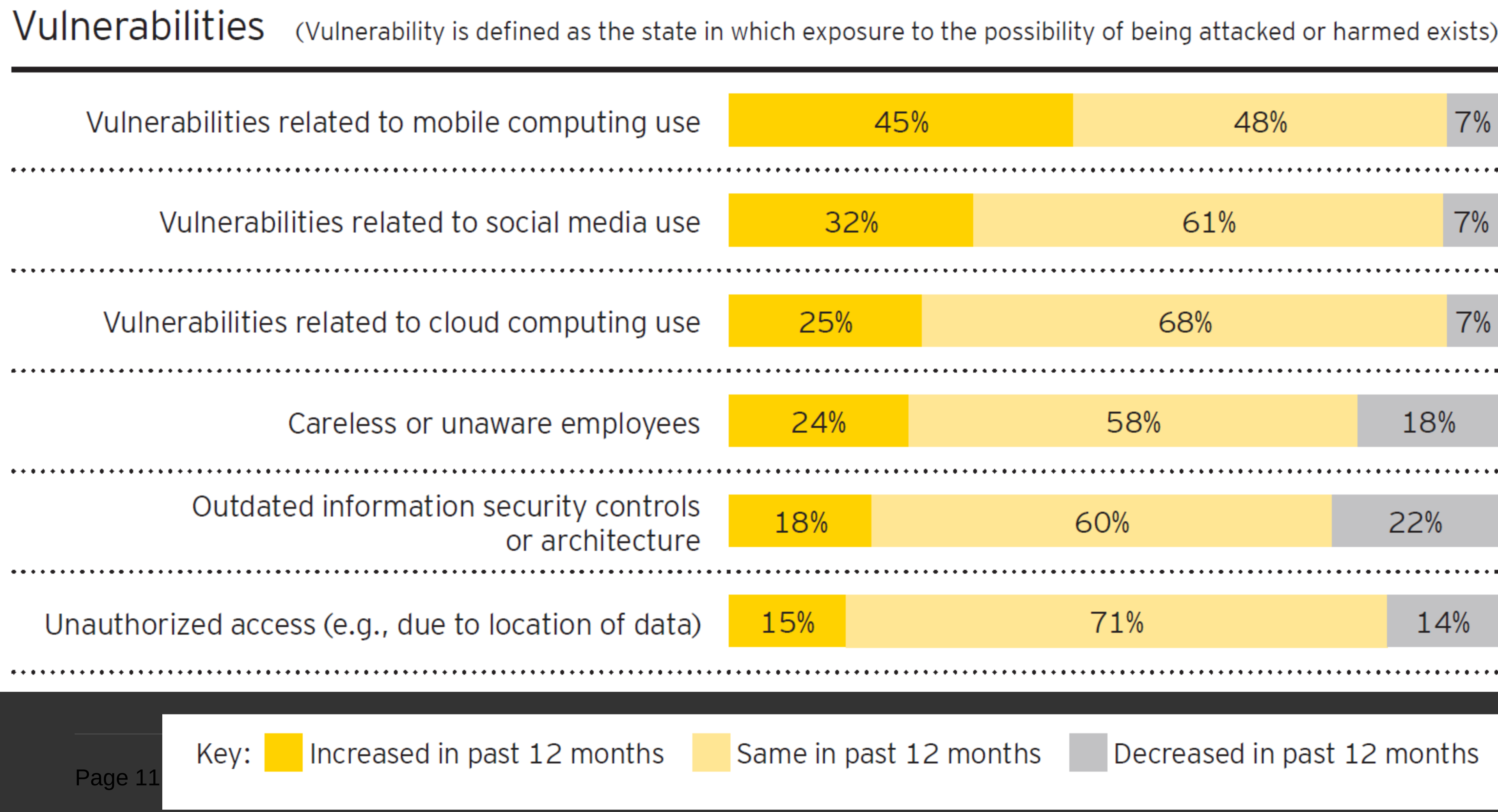
Results shown on a scale of 5 to 1, where 5 is very mature and 1 is nonexistent

Which infosec areas defined as "top priorities" over next 12 months?



Survey respondents were asked to mark five items showing their top priority with a 1, down to their fifth priority with a 5

Vulnerabilities which have most impacted risk exposure over last 12 months



Mobile risk

- The increased use of mobile computing devices for business purposes poses serious risk
- Popularity and widespread use of these devices has led to the unwanted, but predictable results:
  - a target for computer viruses and sophisticated mobile malware
  - due to the small size of the portable devices, simple theft
- The most serious risk of mobile computing is the potential loss or leakage of important business information.
- Survey participants indicated data risk in their top five areas of IT risk
  - 2nd only to continuous availability

Social media

- Protecting data across applications, networks and mobile devices is complex enough
  - social networking by employees is presenting organisations with new and growing frontier of risk.
- The risks, from an information security perspective
  - the loss or leaking of information
  - statements or information that could damage the company’s reputation
  - activity such as downloading pirated material with legal and liability implications
  - identity theft that directly and indirectly compromises the company’s network and information; and
  - data aggregation in building up a picture of an individual to mount security attacks through social engineering.
- Few companies are adequately prepared to counter this threat
  - 60% haven’t implemented security technologies supporting Web 2.0 exchanges such as social networks, blogs or wikis
  - 77% have not established security policies that address the use of social networks or Web 2.0
  - a critical strategy that costs virtually nothing

Controlling social media

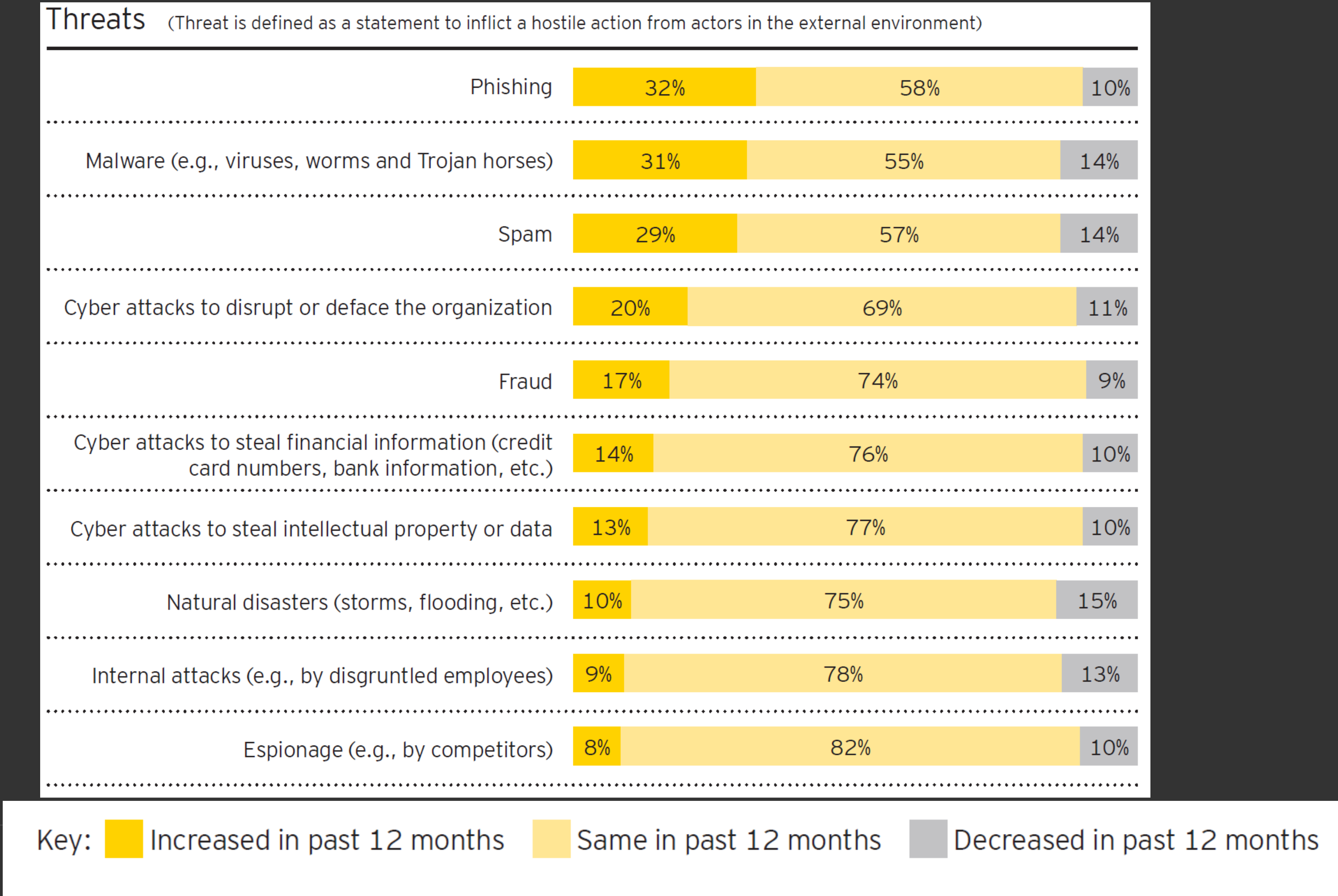
- The simplest way to reduce the risks associated with social networking and Web 2.0 is to restrict or limit the use of such tools in the work environment.
- It is ***doubtful*** that such an approach can be ***successful***
  - it does not prevent the sharing of sensitive information from personal devices or home computers;
  - it could also drive additional unwanted behaviors, such as connecting personal laptops to the business network.

Controlling social media …

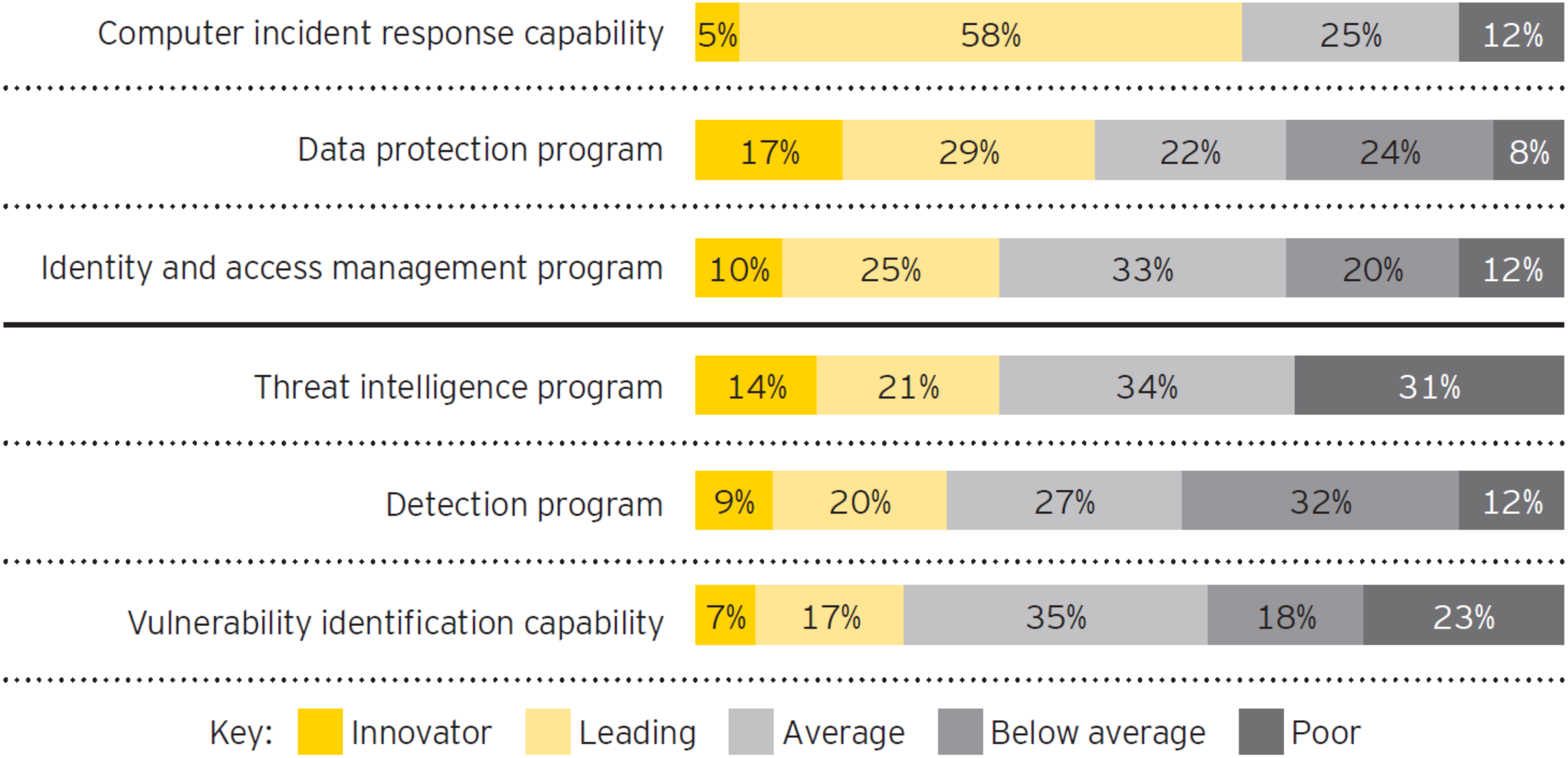
Another downside to such an approach is that the organizations that do not offer or that restrict the use of these tools may be unable to attract and retain the best and brightest from the new generation of workers.

- To create a secure and successful business environment, organizations must involve their people; a technology-savvy workforce will find a way around controls, unless they fully understand the danger of the risks involved.
- By informing every member of the organization on the risks and issues related to social media, information security becomes an expanded function that all employees are fully aware of and have a responsibility to perform.

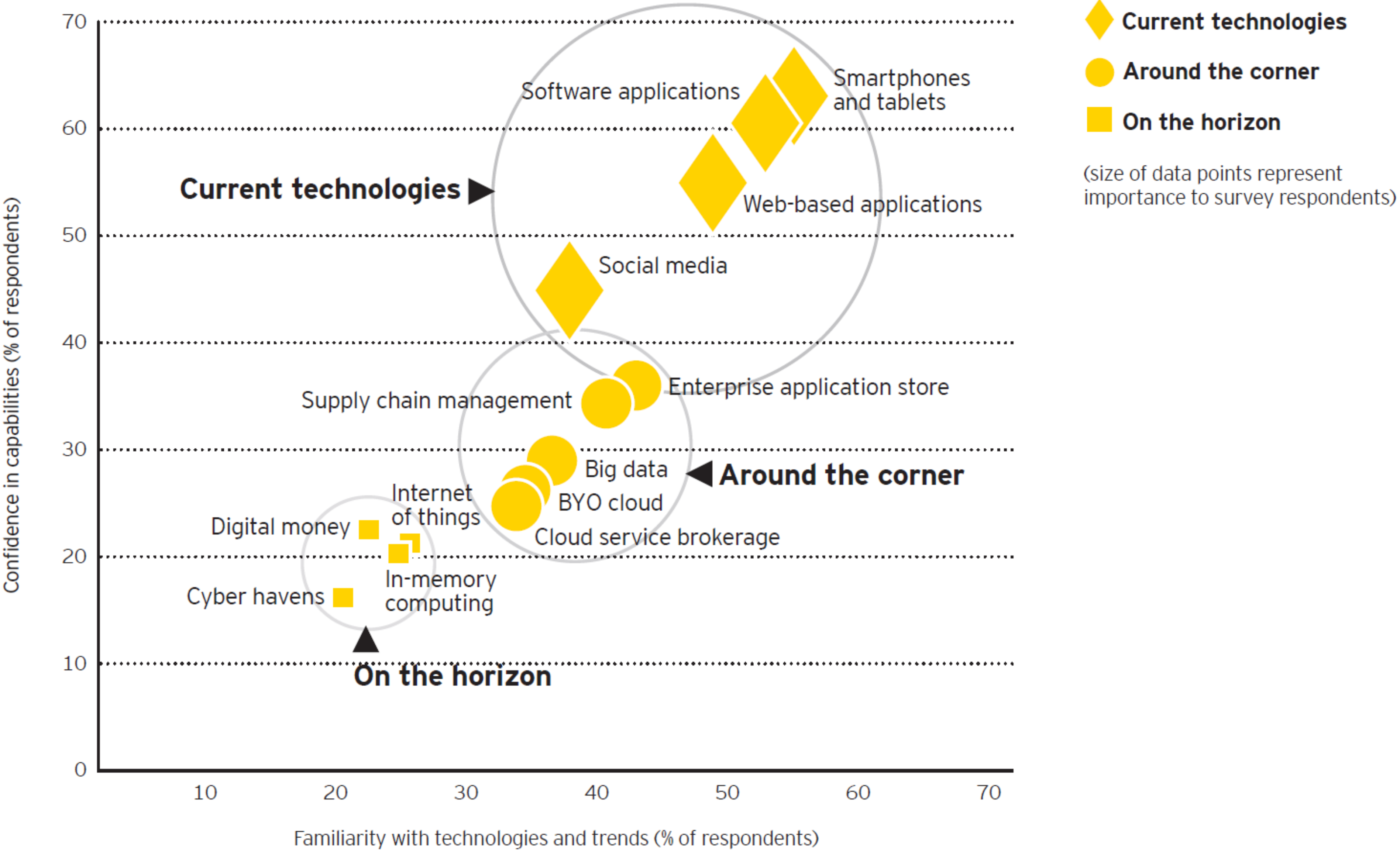
Threats which have most impacted risk exposure over last 12 months



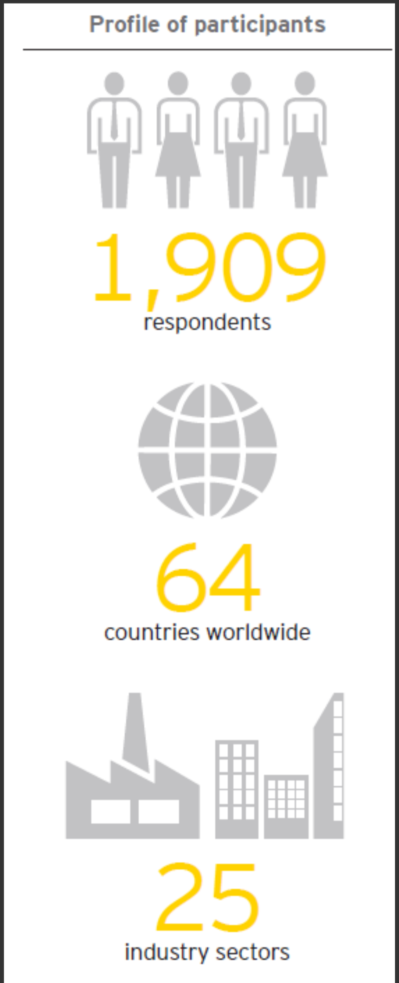
Infosec programme maturity



Emerging technologies and trends



Profile of participants

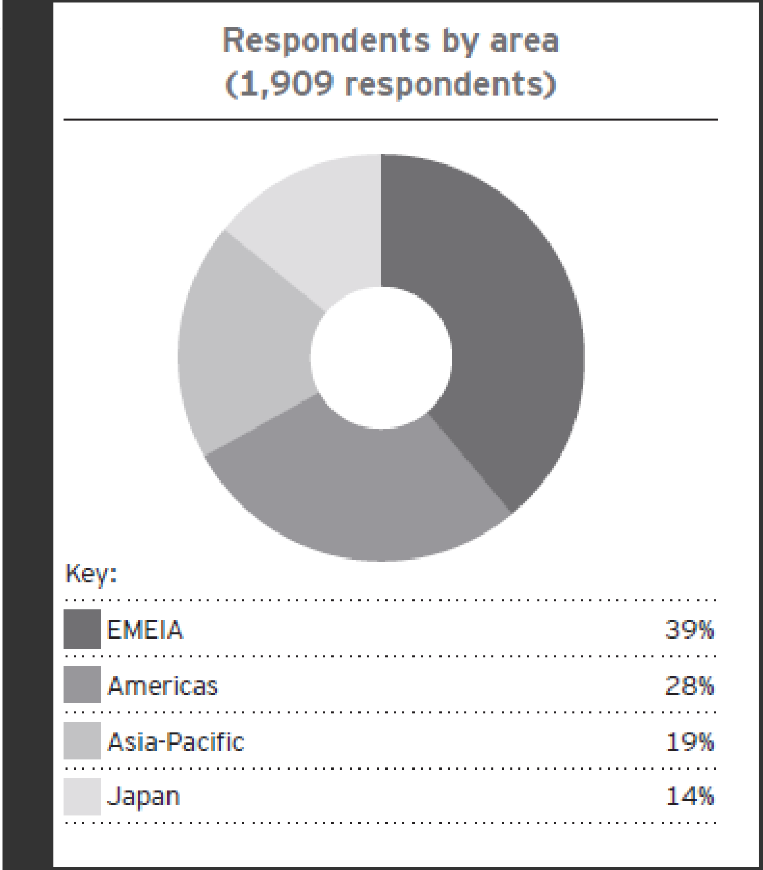


Profile of participants

1,909
respondents

64
countries worldwide

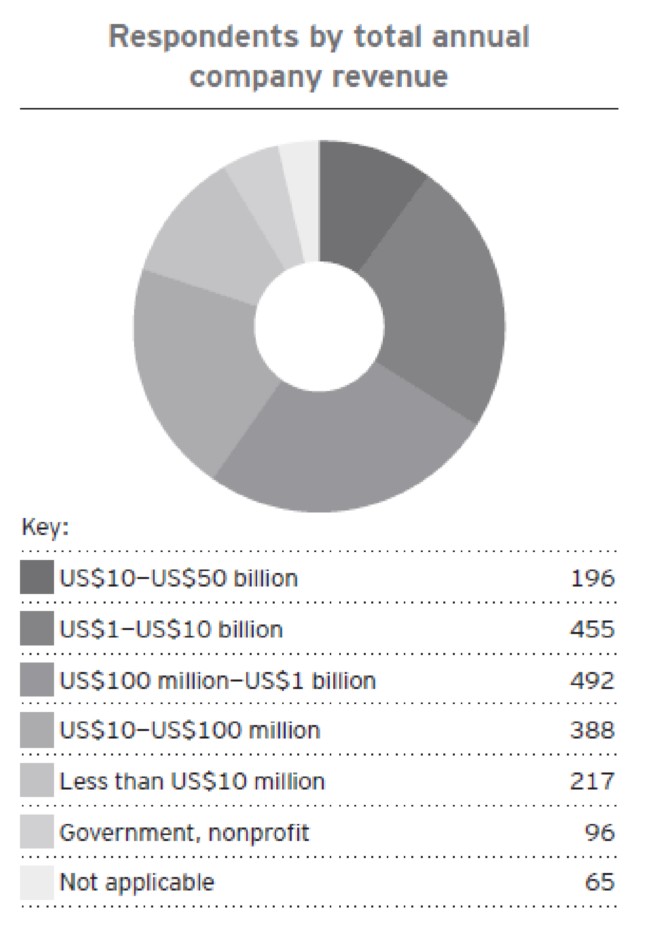
25
industry sectors



Respondents by area
(1,909 respondents)

Key:

■	EMEIA	39%
■	Americas	28%
■	Asia-Pacific	19%
■	Japan	14%



Respondents by total annual company revenue

Key:

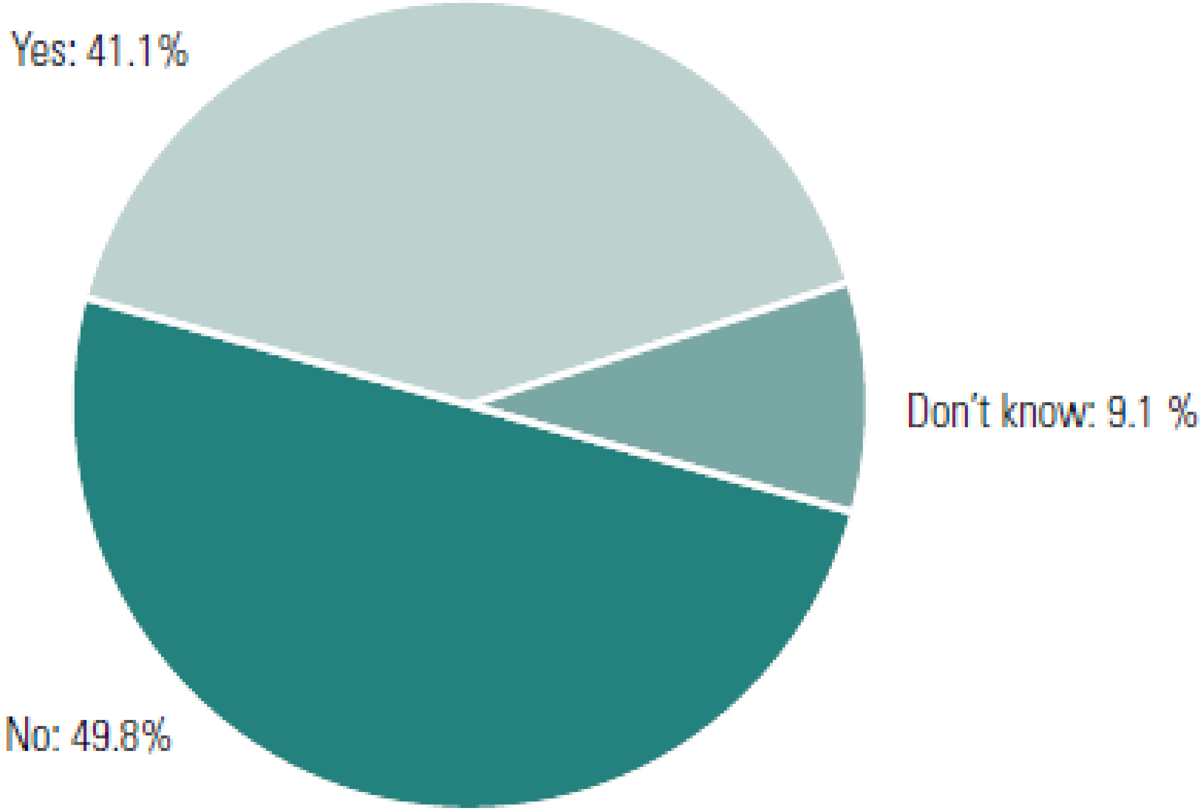
■	US$10–US$50 billion	196
■	US$1–US$10 billion	455
■	US$100 million–US$1 billion	492
■	US$10–US$100 million	388
■	Less than US$10 million	217
■	Government, nonprofit	96
■	Not applicable	65

2010/11 CSI Computer Crime & Security Survey

- Malware infection most common attack, 67.1% reported
- Half the respondents experienced at least one incident
  - 45.6% of these were targeted attacks
- Fewer respondents than ever willing to share specific information about financial losses they incurred.
- Regulatory compliance efforts had a positive effect on security programs
- Respondents did not believe malicious insiders accounted for much of their losses due to cybercrime

- Survey
  - 351 computer security practitioners in the USA
  - 15th year of survey
  - www.gocsi.com

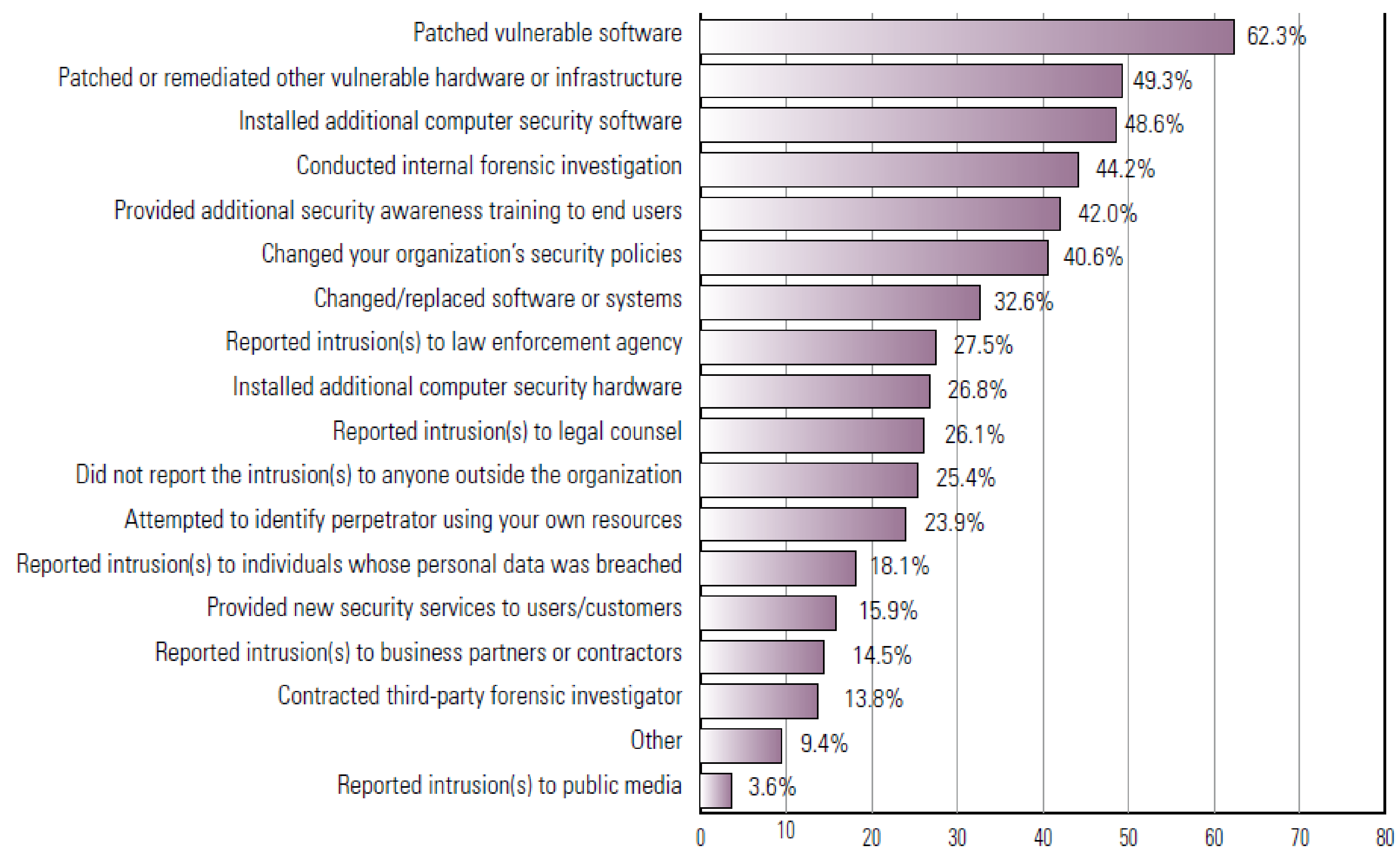
CSI 2010/11 Survey:Experienced Security Incident



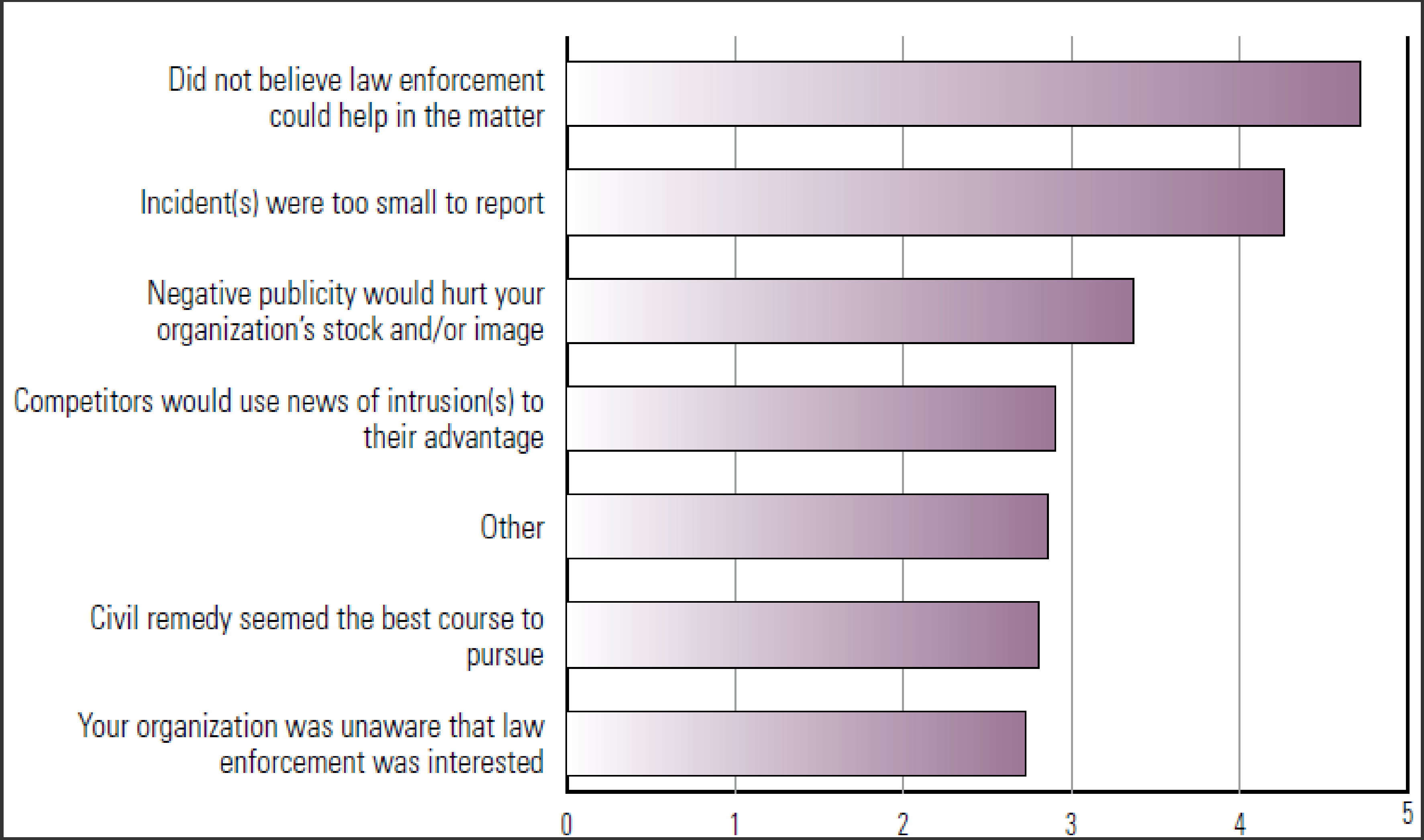
2010 CSI Computer Crime and Security Survey

2010: 285 Respondents

CSI 2010/11 : Actions taken after incident



CSI 2010/11 Survey : Why not report



Cost of computer security breaches

- 80% of organisations acknowledged financial loss as a result of a computer breach. (2008)
- 44% were willing and/or able to quantify their financial loss
- Most serious financial loss as a result of theft of proprietary information and financial fraud
  - Theft of proprietary information and financial fraud account for 2/3 of financial losses
  - Yet, only 20% report incidents of theft of proprietary info and only 12% report incidents of financial fraud

Cost of computer security breaches …

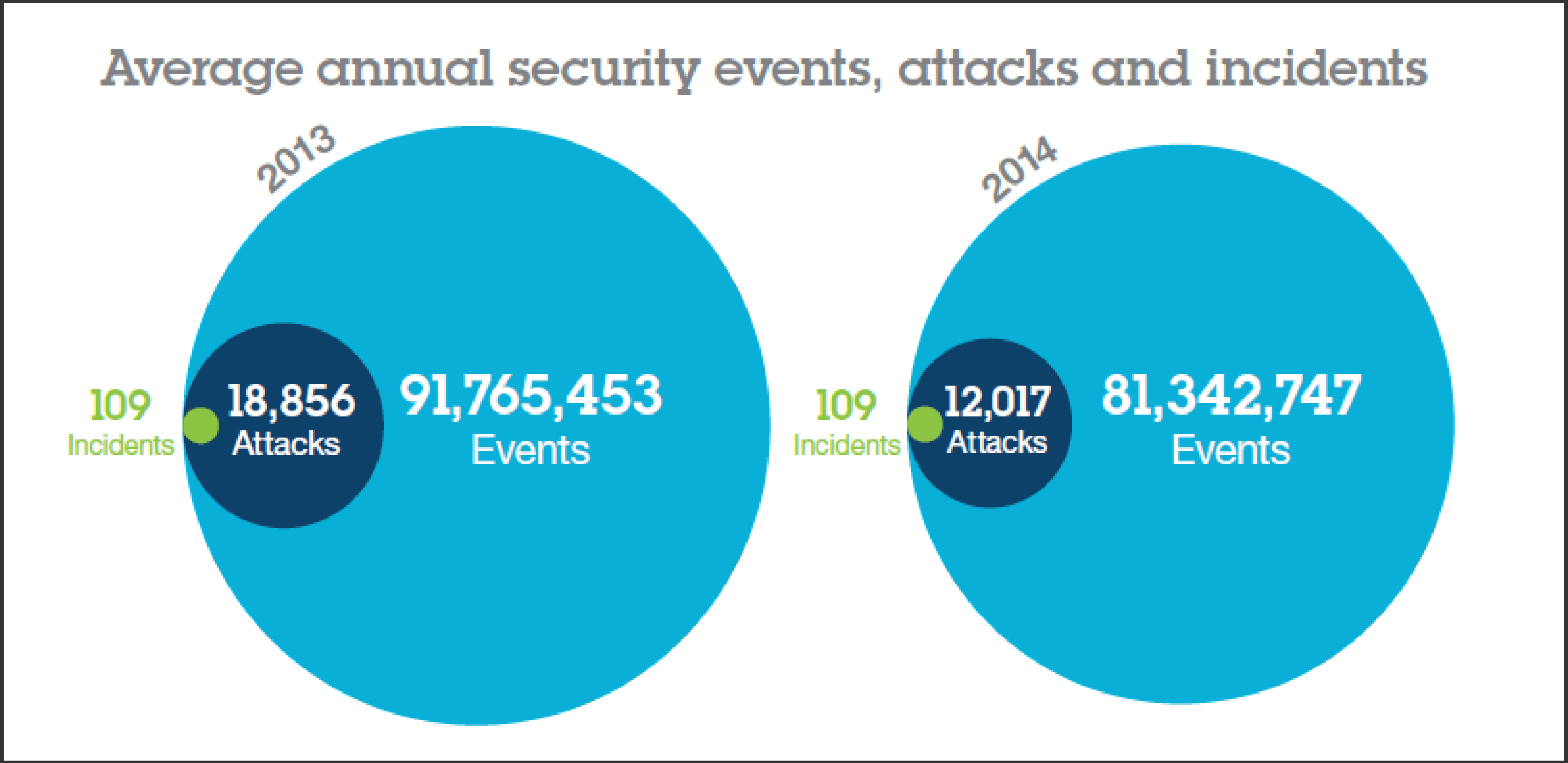
- Trend moved downwards (per CSI/FBI)
  - Insufficient data to report in 2010/11
  - $289k average incident loss (2008), still down from early 2000’s
  - Highest Average loss $3,149k in 2001

- Other
  - In South Africa, the average loss per incident is over R575 000 (from KPMG’s 2002 security survey)
  - RIAA won $1million settlement from IIS - employees ran INTERNAL server for MP3’s
  - Biggest concern is reputation damage (Ernst & Young 2008 survey)

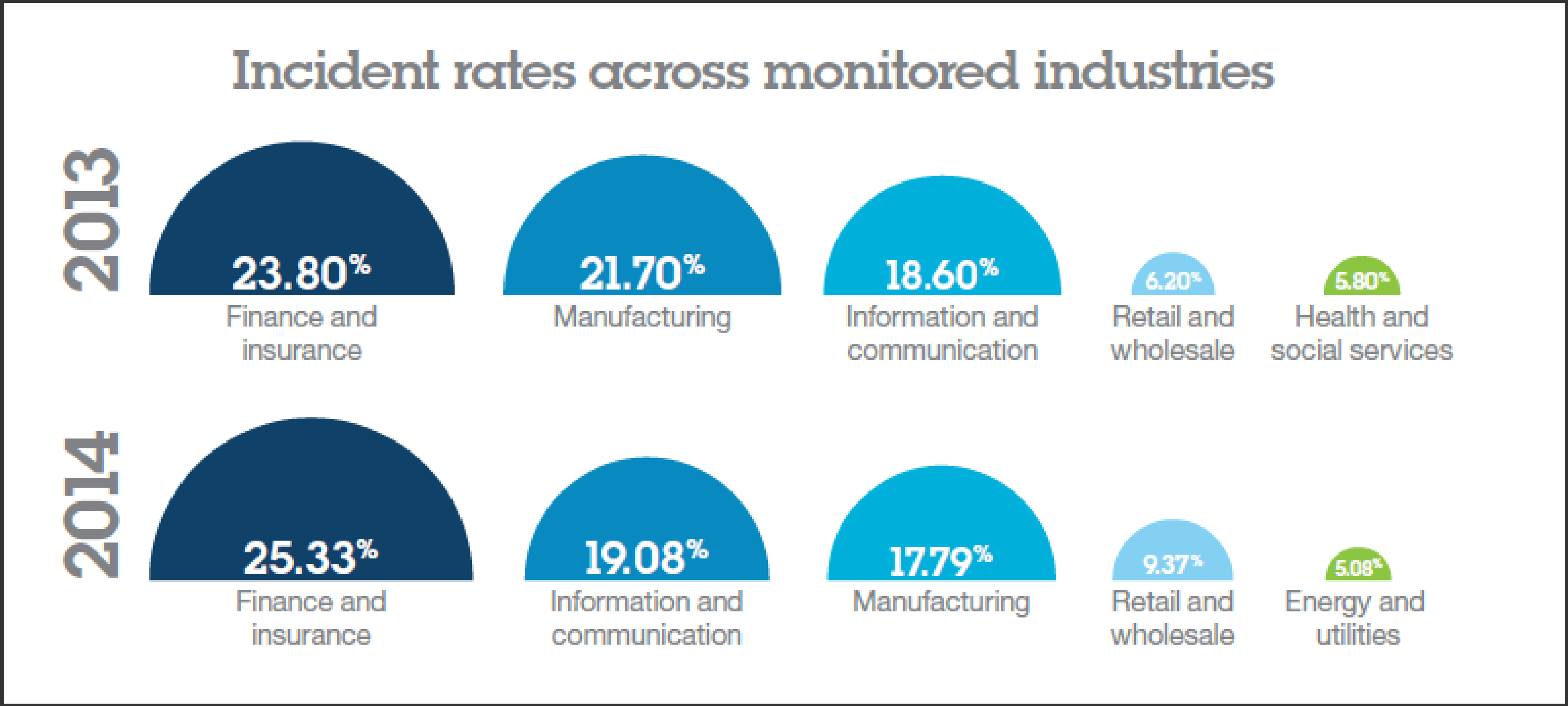
Cybercrime in SA (IBM 2015)

- Cybercrime in South Africa
  - One billion pieces of personal data lost in SA in 2014
  - Cyber related cost of R432 256 000 (2014)
  - Costs in 2015 already R465 412 000
- Incident related costs
  - Lost business R19,279m
  - Forensic investigation R12,157m
  - Cost per lost record R2088

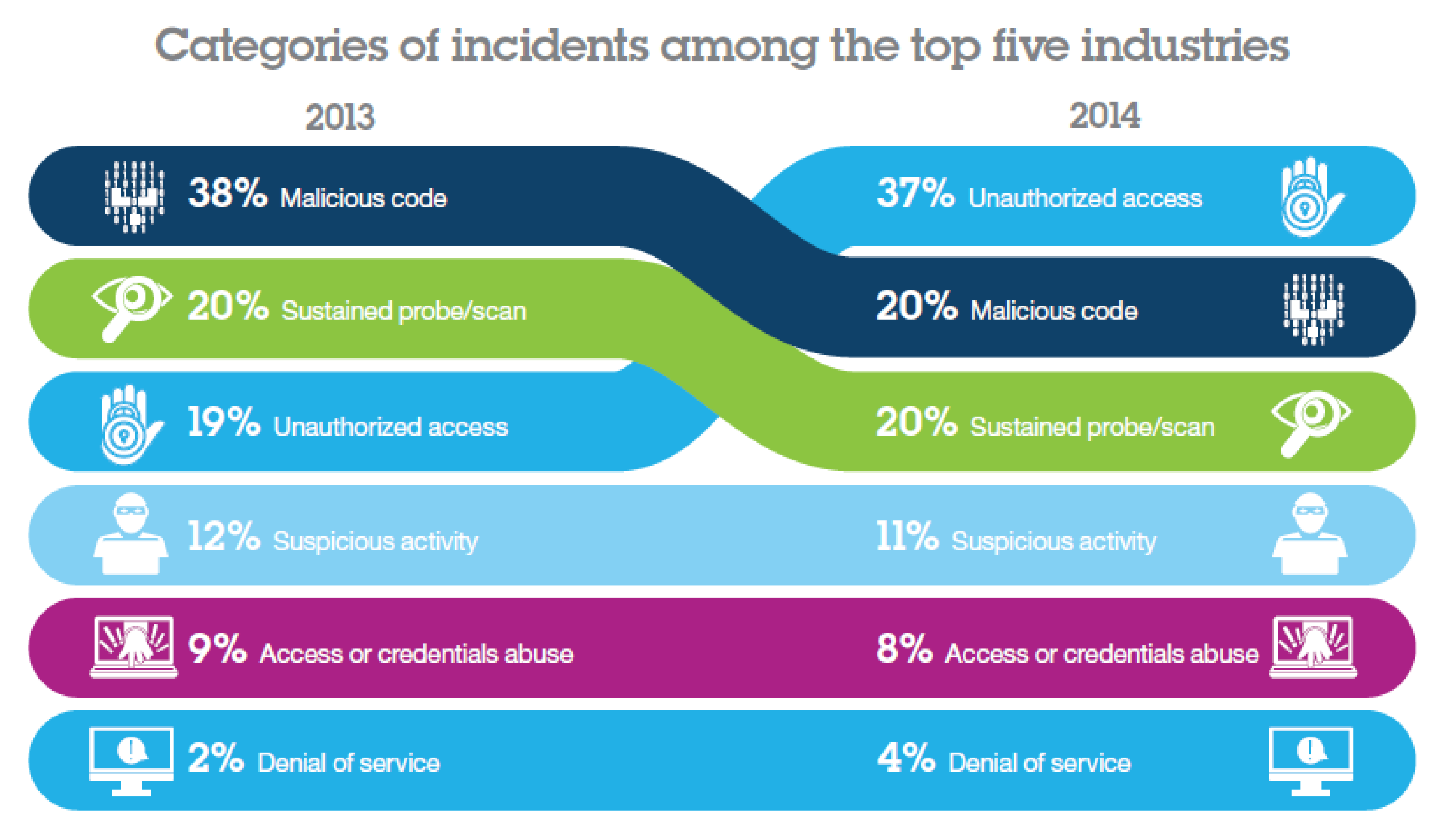
Cybercrime in SA (IBM 2015)



Cybercrime in SA (IBM 2015)

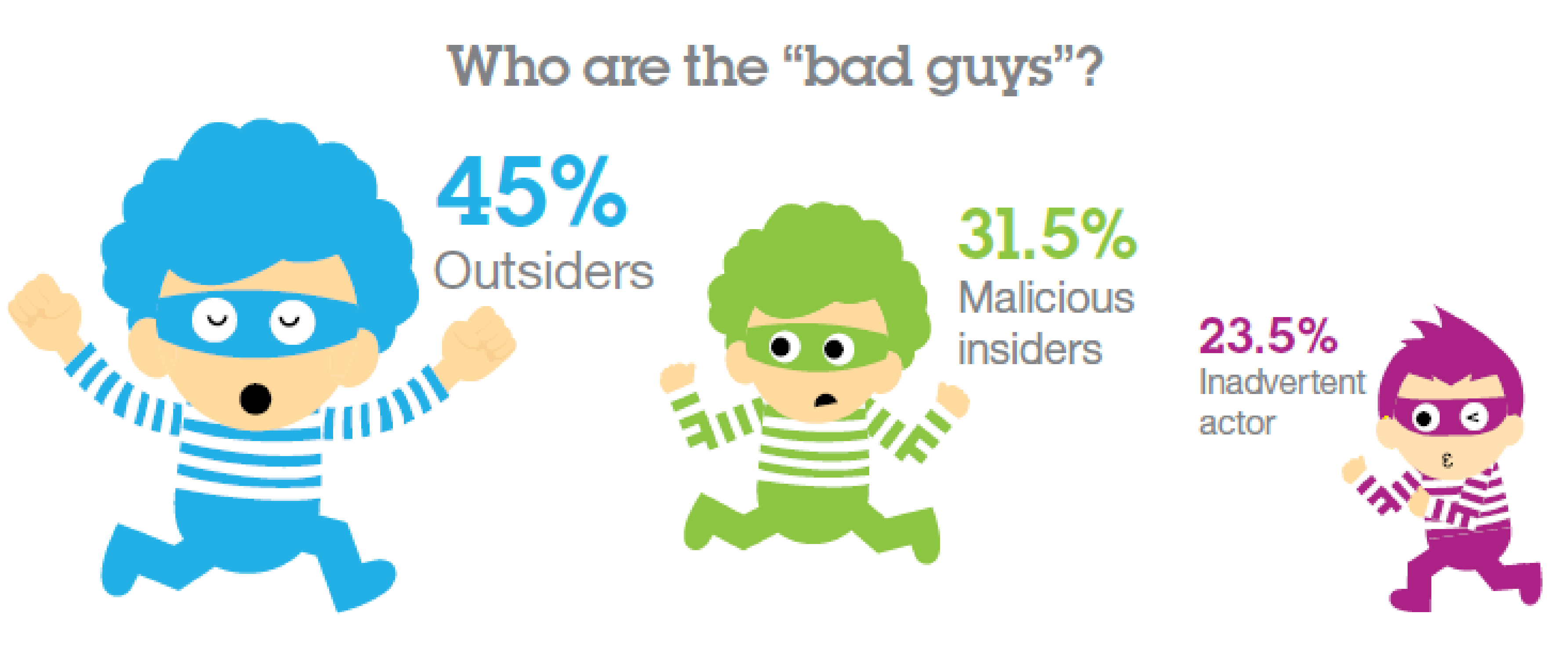


Cybercrime in SA (IBM 2015)

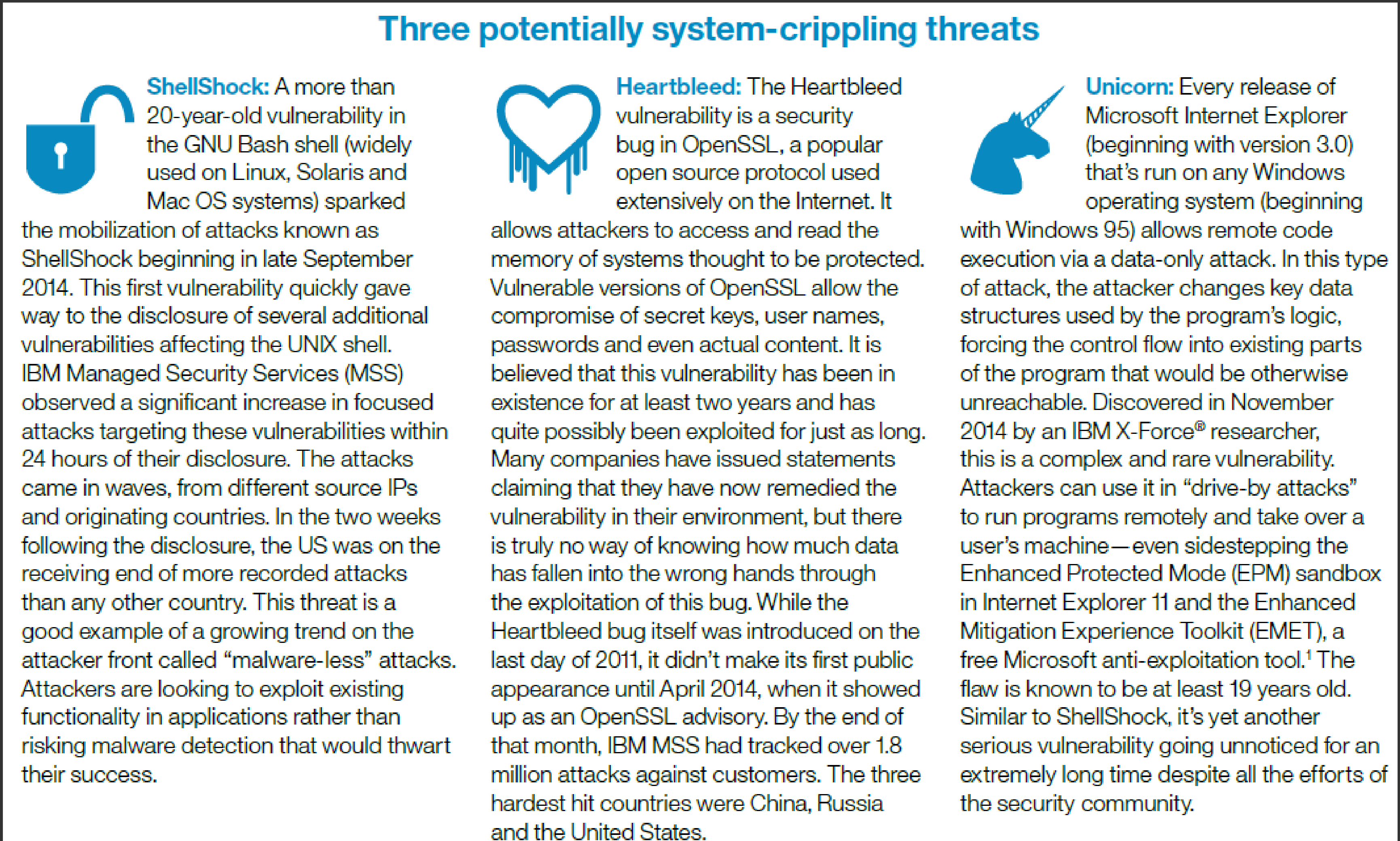


P

Cybercrime in SA (IBM 2015)



Cybercrime in SA (IBM 2015)



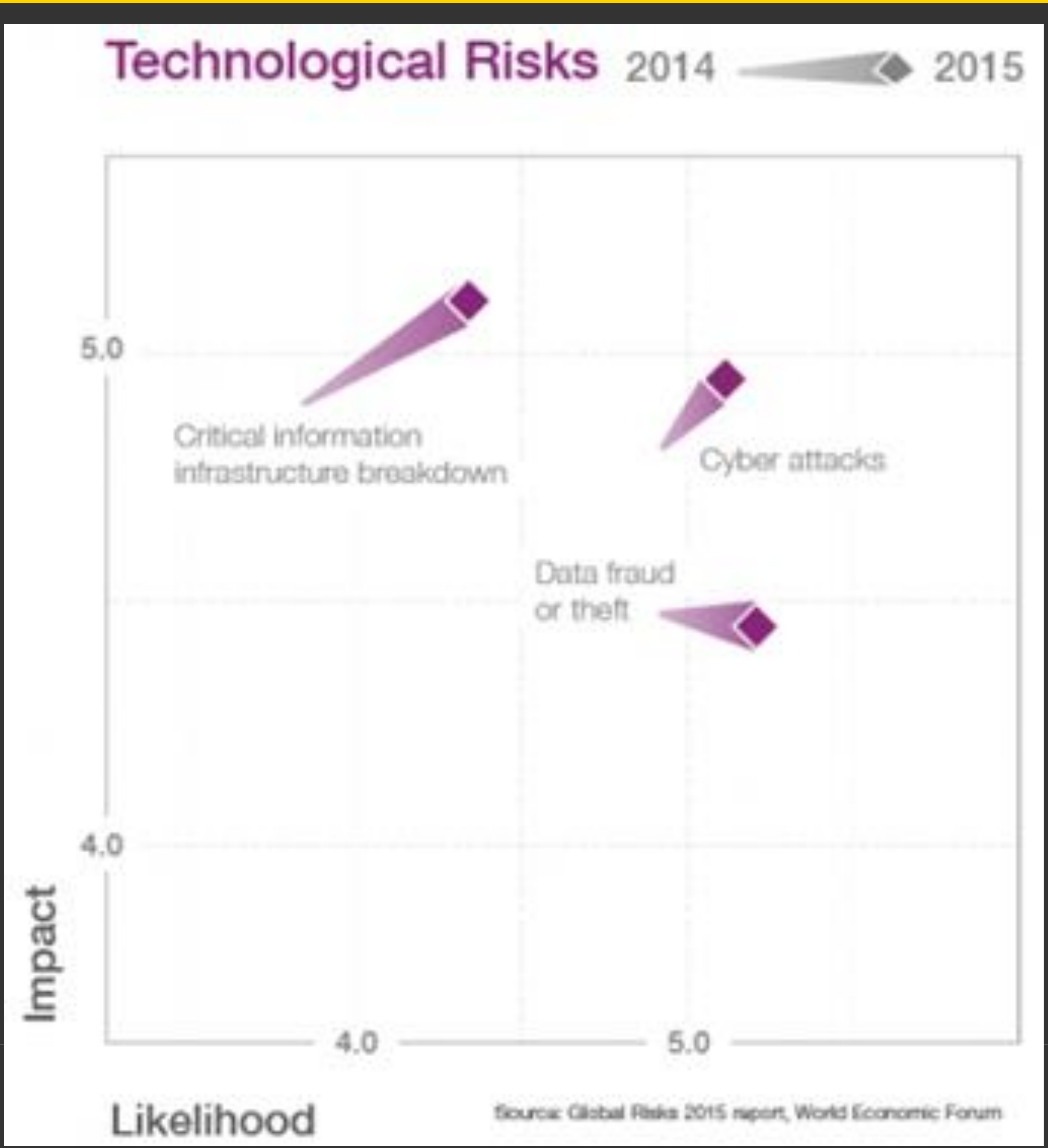
Three potentially system-crippling threats

ShellShock: A more than 20-year-old vulnerability in the GNU Bash shell (widely used on Linux, Solaris and Mac OS systems) sparked the mobilization of attacks known as ShellShock beginning in late September 2014. This first vulnerability quickly gave way to the disclosure of several additional vulnerabilities affecting the UNIX shell. IBM Managed Security Services (MSS) observed a significant increase in focused attacks targeting these vulnerabilities within 24 hours of their disclosure. The attacks came in waves, from different source IPs and originating countries. In the two weeks following the disclosure, the US was on the receiving end of more recorded attacks than any other country. This threat is a good example of a growing trend on the attacker front called "malware-less" attacks. Attackers are looking to exploit existing functionality in applications rather than risking malware detection that would thwart their success.

Heartbleed: The Heartbleed vulnerability is a security bug in OpenSSL, a popular open source protocol used extensively on the Internet. It allows attackers to access and read the memory of systems thought to be protected. Vulnerable versions of OpenSSL allow the compromise of secret keys, user names, passwords and even actual content. It is believed that this vulnerability has been in existence for at least two years and has quite possibly been exploited for just as long. Many companies have issued statements claiming that they have now remedied the vulnerability in their environment, but there is truly no way of knowing how much data has fallen into the wrong hands through the exploitation of this bug. While the Heartbleed bug itself was introduced on the last day of 2011, it didn't make its first public appearance until April 2014, when it showed up as an OpenSSL advisory. By the end of that month, IBM MSS had tracked over 1.8 million attacks against customers. The three hardest hit countries were China, Russia and the United States.

Unicorn: Every release of Microsoft Internet Explorer (beginning with version 3.0) that's run on any Windows operating system (beginning with Windows 95) allows remote code execution via a data-only attack. In this type of attack, the attacker changes key data structures used by the program's logic, forcing the control flow into existing parts of the program that would be otherwise unreachable. Discovered in November 2014 by an IBM X-Force® researcher, this is a complex and rare vulnerability. Attackers can use it in "drive-by attacks" to run programs remotely and take over a user's machine—even sidestepping the Enhanced Protected Mode (EPM) sandbox in Internet Explorer 11 and the Enhanced Mitigation Experience Toolkit (EMET), a free Microsoft anti-exploitation tool.[1] The flaw is known to be at least 19 years old. Similar to ShellShock, it's yet another serious vulnerability going unnoticed for an extremely long time despite all the efforts of the security community.

World Economic Forum Global Risk 2015



Source: Global Risks 2015 report, World Economic Forum

BEATTIE
©99 Daytona Beach Sunday News-Journal

"The virus was contained in an e-mail warning about the virus . . ."

Current happenings

What's going on out there
In the REAL world

Right NOW!

Could it be the biggest infosec failure of the decade?

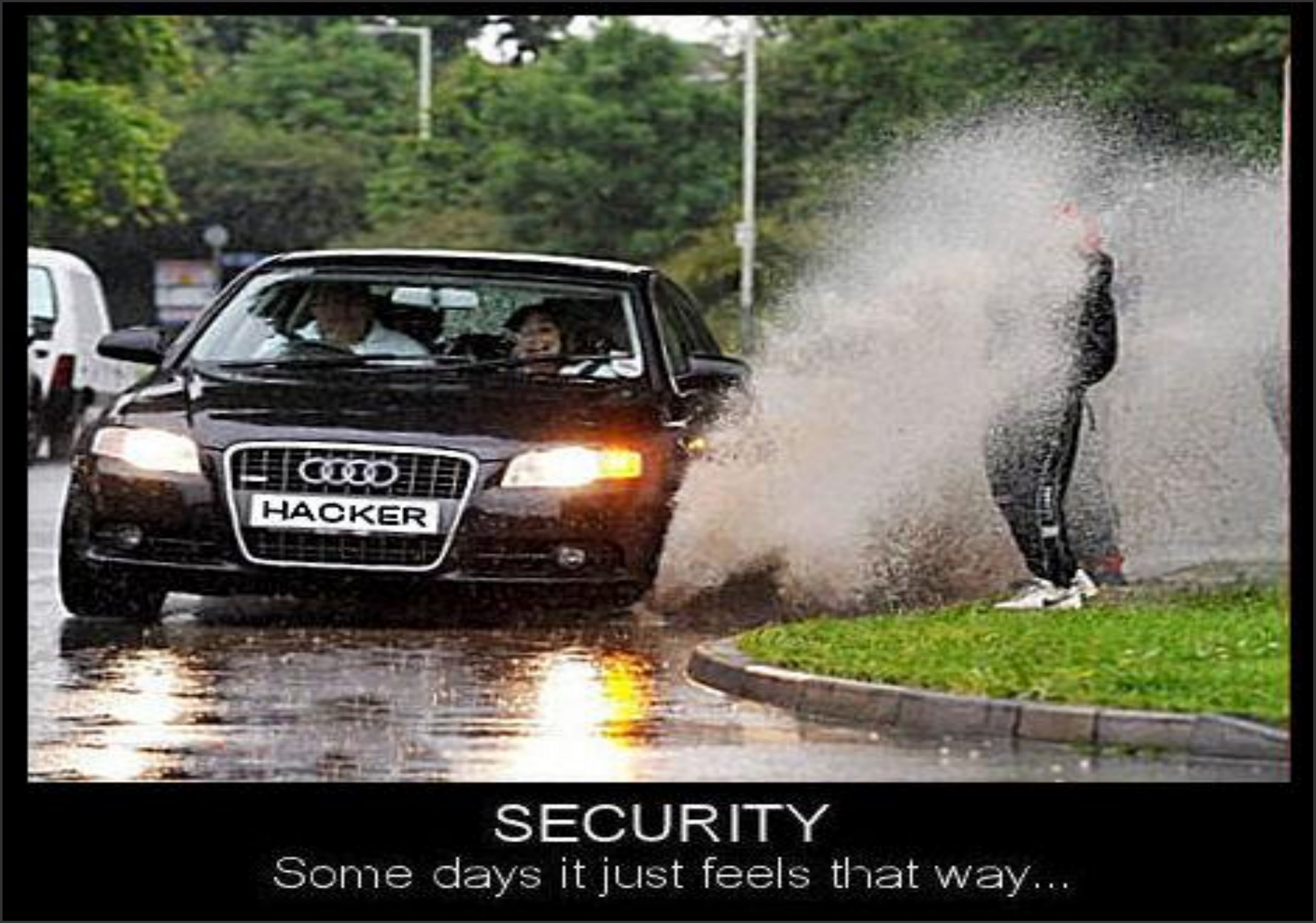
- Who is it?

Sony: The Company That Kicked the Hornet's Nest

Biggest failure of the decade?

- An April 2011 hacking incident that targeted its PlayStation and Sony Online Entertainment networks
- 100 million people use to play video games, watch movies, and listen to music online.
- The attack resulted in the second-largest data breach in U.S. history, exposing records including credit-card numbers and
- forcing Sony to pull the plug on the networks indefinitely.
- Sony hopes to have them back online by the end of May.
- A full accounting of the disaster, both in dollar terms and in damage to the PlayStation brand, will take months, if not years.

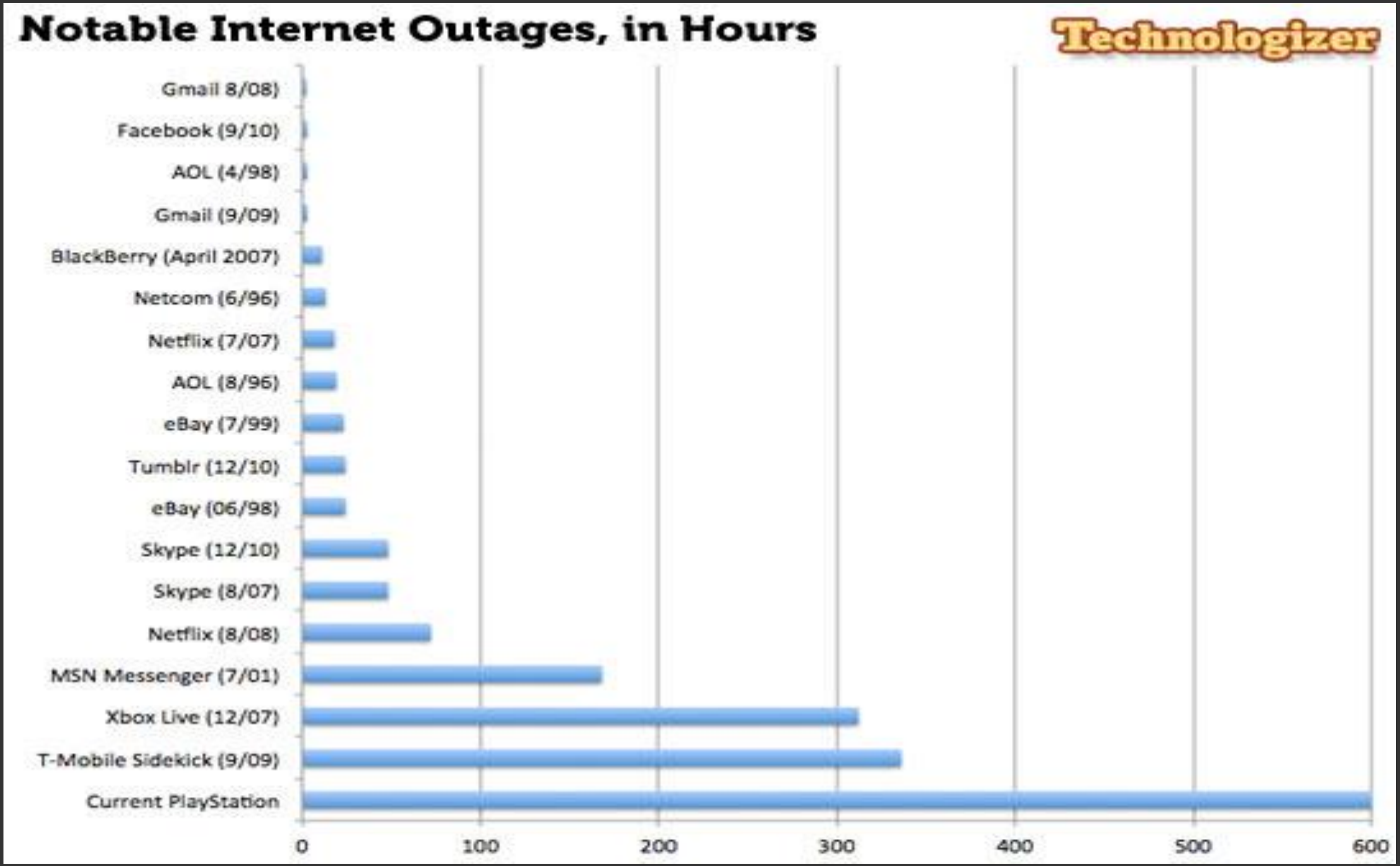
How they feeling



SECURITY

Some days it just feels that way...

Comparative outages



The Streisand effect

“It happens when a person or company tries to suppress a piece of information and, in so doing, unintentionally popularizes it.”

- A site hosted picture of the house of Barbara Streisand – nobody really cared
- She unsuccessfully sued for removal
- The publicity drew many more people to the pictures than ever would have otherside

Source : Bloomberg Business Week

The Sony Effect

- In the future, a blowback in the realm of cybersecurity might be known as the Sony Effect.
- Sony may have unintentionally brought the crisis on itself
- other tech companies have worked to establish an uneasy truce with hackers
  - Sony has antagonized them with lawsuits and prosecutions
  - At the same time, security experts say Sony essentially left the keys in the car
  - ailing to adequately protect or even monitor crucial parts of its server infrastructure

"They appeared to be operating in an environment where no one had really assessed the risks," says Eugene H. Spafford in his congressional hearing.

How it started?

- Mr George Hotz (GeoHot)

A quick and biased history

- Geohot hacked the iphone when he was 17
  - Apple and hackers been in cat and mouse game ever since with each new release of iOS
- PS3 was unhackable, Sony was arrogant
- GeoHot claimed everything is hackable
- The world laughed
- He hacked the PS3, met with disbelief
  - How?
  - Intentional hardware glitch

A quick and biased history ..

- Sony responds by removing OtherOS (Linux) from the PS3, prompting global outrage and lawsuits
- GeoHot promises a hacked firmware to bring it back but never delivers
- GeoHot found other vulnerabilities, published them online
  - Sony sued him to take down
  - Seized his computers, twitter account, PayPal records

A quick and biased history ..

- "Trying to sue a member in good standing out of existence didn't do them any favours" says Dave Aitel, white-hat hacker.
- Anonymous vows to retaliate
  - They are the hacker collective that brought down the websites of MasterCard and other payments processors in December
- German police raid apartment of Alexander Egorenkov, another hacker who distributed software that let PlayStation consoles run homemade games
- Other tech companies found ways to channel hackers
  - Microsoft after initial wobbly let hackers play with Kinect
  - Google pays for bugs found in it’s software
- Sony wasn’t very good at listening about flaws in it’s systems
- Sony settled with GeoHot on 31 March 2011, very biased settlement against Geohot

A quick and biased history …

- Penetration scanning software began scanning Sony's PlayStation Network at 7:09 a.m. on March 3rd 2011
  - McDanel knows this because Sony left one of its server logs, which record all the activity performed by a machine, completely unguarded on the open Web
- the probers used an off-the-shelf program that is easy to obtain and not very stealthy
- Anyone checking the server logs would have been able to recognize its tell-tale signs and prevent the break-in
- Sony was "negligent" for not doing so
- On April 15 2011, after six weeks of scanning, the penetration software suddenly stopped
- most likely because "they found what they had been looking for, a vulnerability in the network,“
- Four days later, Sony noticed the first signs of a break-in

A quick and biased history …

- Company spokesman
  - “Sony was the victim of a highly sophisticated attack and that the company's network had multiple security measures in place."
- No one has taken credit for the attack
  - Sony executives told Congress that they found a file left by the hackers
  - reads "We are legion"—the motto of Anonymous.

Whoever the culprit may be, Sony now has good reason to familiarize itself with the mechanics of the Streisand Effect. After all, it owns Streisand's label.

***The bottom line:** Security experts say Sony should have recognized the warning signs of an impending attack, which compromised 100 million accounts.*

Amazon hacked Sony!

- Amazon’s Web Services cloud computing unit was used by hackers in last month’s attack against Sony’s online entertainment systems, according to a person with knowledge of the matter
  - using an alias signed up to rent a server through Amazon’s EC2 service
  - launched the attack from there
  - Hackers didn’t break into Amazon’s servers, just signed up using fake information
- sheds light on how hackers used the so- called cloud to carry out the second-biggest online theft of personal information to date
- The FBI will likely subpoena Amazon or try get a search warrant
- Drew Herdener, a spokesman for Seattle-based Amazon, declined to comment. Amazon didn’t respond to a request to speak with Chief Executive Officer Jeff Bezos
- “The use of a hijacked or rented server to launch attacks is typical for sophisticated hackers. The proliferation of server farms around the globe has made such misdirection easier.” E.J. Hilbert, president of Online Intelligence, former FBI cyber-crime investigator.

Source : Bloomberg.net

More on hacking with Amazon

- German hacker used rented computing resources to crack a secure hashed password
- Used GPU-based rentable resource to brute crack SHA1 hashes
  - used in SSL, Transport Layer Security and S/MIME protocols)
- used the Cuda-Multiforcer tool
- Cost just $2
- All 1-6 character passwords cracked in 49m (on the fly, not using rainbow tables)
  - Used to take distributed computing projects worldwide months
- Moxie Marlinspike's online Wi-Fi password-cracking service (WPAcracker.com)
  - $17-a-time service to crack Wi-Fi password in around 20m
  - 120 hours for dual-core PC to do same
- More details here : http://stacksmashing.net/2010/11/15/cracking-in-the-cloud-amazons-new-ec2-gpu-instances

President apologises

President and CEO Kazuo Hirai (center,) senior vp Shiro Kambe (left) Shinji Hasejima (right), start of press conf May 1 at the Sony Corp. headquarters in Tokyo. They bowed in apology for a security breach in the company’s PlayStation Network that caused the loss of personal data of some 77 million accounts on the online service

What is the impact of the hack?

- Financial on Sony development partners
  - Q-Games' Dylan Cuthbert (PixelJunk) tells Industry Gamers the outage "definitely" impacts his studio financially, and says he believes Sony is "running around patching holes," but that it may be several weeks before the company has "something more concrete to say."
  - Activision warned that it expects quarterly revenue to dip year-on-year because of a smaller product lineup, but also because of "the expected loss of high-margin revenue due to the temporary PlayStation Network shutdown."
  - it costs Capcom "hundreds of thousands, if not millions of dollars in revenue

  Will Sony compensate developers?
  - Q-Games' Cuthbert hopes so, telling Industry Gamers he has a "feeling" Sony's thinking about it, lest they "lose developers which of course is pretty bad for them."

Source : PC World

Impact of hack continued …

- Sony compensates users
  - 2 free games to every Playstation 3 user
  - 2 free games to every PSP user
  - 1 month free premium service (or 1 month extension) to all users
- USA users only
  - offer a $ 1 million insurance policy per user
    - covering legal expenses,
    - identity-restoration costs and
    - lost wages that occur after data is stolen
  - Subscribers have until June 18 to sign up for Debix's AllClear ID Plus protection program
- The rest of us?

Impact of hack continued …

- Sony could face heavy penalties if falls foul of UK data standards
- “Under the Data Protection Act, there are principles that regulate how companies that collect personal data should manage and use that data, and one of them is that they have to take appropriate technological safeguards to protect that data,” Simon Halberstam, partner at London law firm Kingsley Napley LLP
- “If they fell below what’s regarded as best practice in terms of the technological safeguards that they took, they would be in breach of the Data Protection Act.”
- “In that case, they are potentially liable, and they could be fined by the Information Commision accordingly.”
- Maximum fine is £500,000
- The UK’s Information Commissioner’s Office confirmed it is taking the PSN breach “seriously” and is due to talk to Sony

Recovery started

- Recovery started on a phased rollout over late June
  - Had to be taken down at times as servers overloaded
  - Was not working in SA despite mails sent out providing details on the recovery
  - Still only partially operational on inconsistent basis
- Japanese government prevent system coming back online in Japan pending further investigation and assurances

More bad news for Sony

- A URL password exploit was identified and corrected after rollout
- Servers had to be taken offline during rollout as they couldn’t cope
- Servers in Thailand were identified as delivering phishing code against Italian CC company
  - “We know you’re not supposed to kick somebody when they are down, but we just found a live phishing site running on one of Sony’s servers..” F-Secure’s Mikko Hypponen
- Thousands of dollars in credits stolen from over a thousand customers’ accounts
- CNET reports PS3 tradein’s up 200% and people are swapping them for XBOX 360’s

Wow. Anybody else got a confession?

- 12th May Eido and Deus Ex website hacked
  - a splinter group of the hacker organisation Anonymous broke through Square Enix security
  - stole personal data of > 80,000 registered users
  - IRC logs show debate to released SRC (4 games?)
- eHarmony (dating site)
  - Hacked and notified in december
  - Argentinian hacker (also hacked PlentyOfFish.com)
  - Hacker and research contacted admins, no response
  - In Feb user database up for sale on Carder.biz
    - Price? $2000 - $3000
  - 10th Feb eHarmony tell users to change passwords?

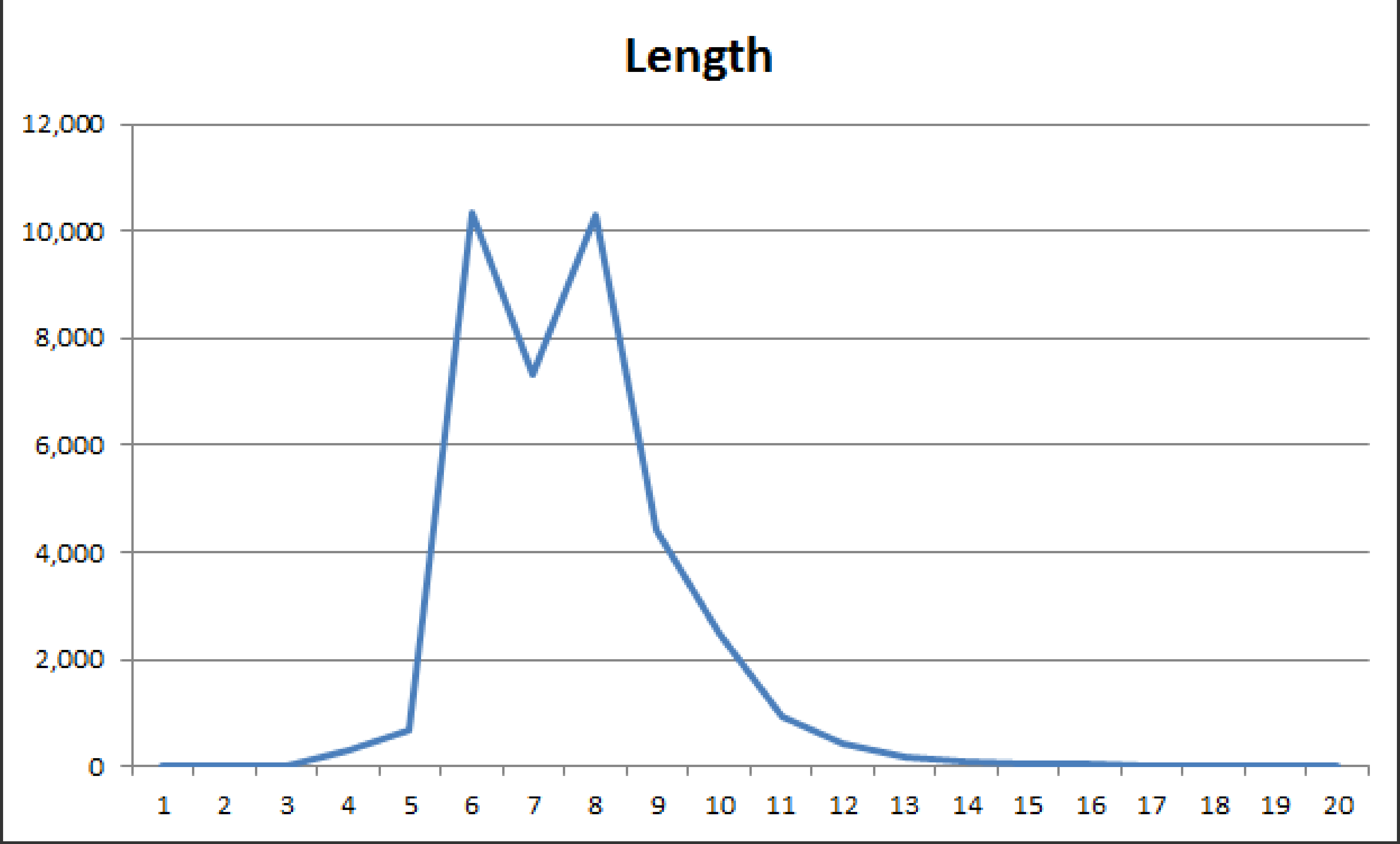
But wait, there is more ....

Analysis of hacked passwords

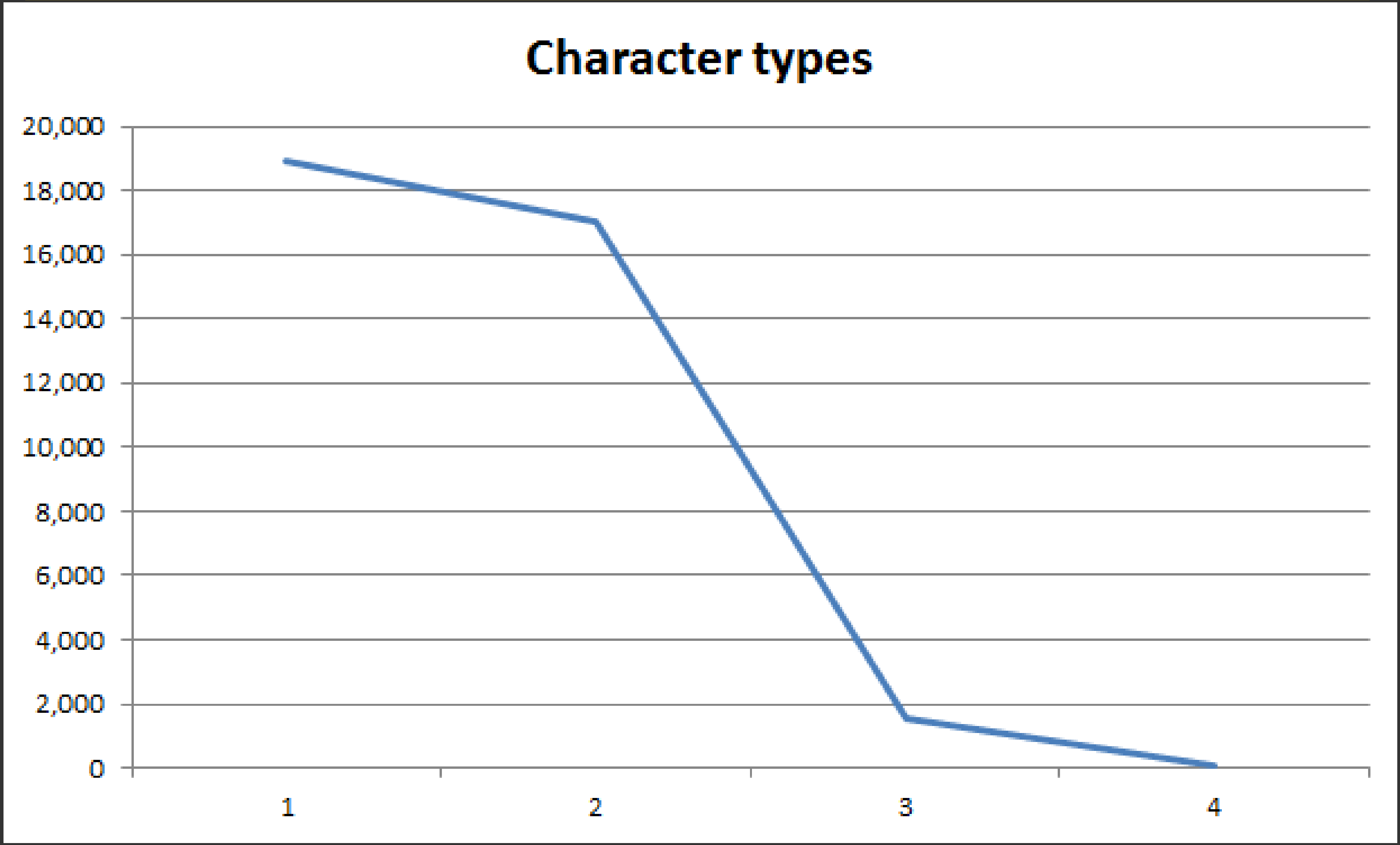
- Troy Hunt analysed password released by Anonymous

- Looked at :
  - Length
  - Variety of Character types
  - Randomness
  - Uniqueness

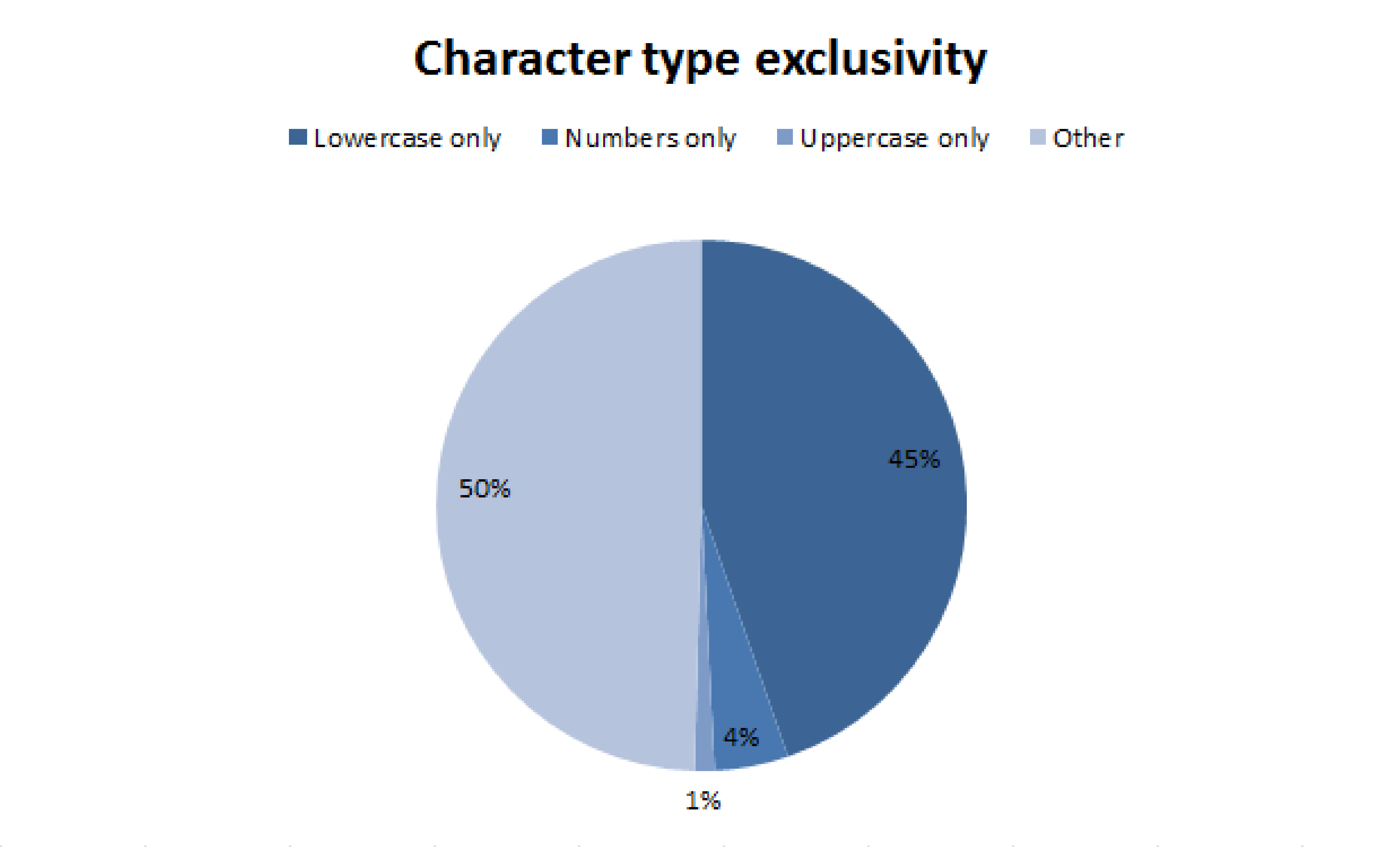
Password Length



Character Types

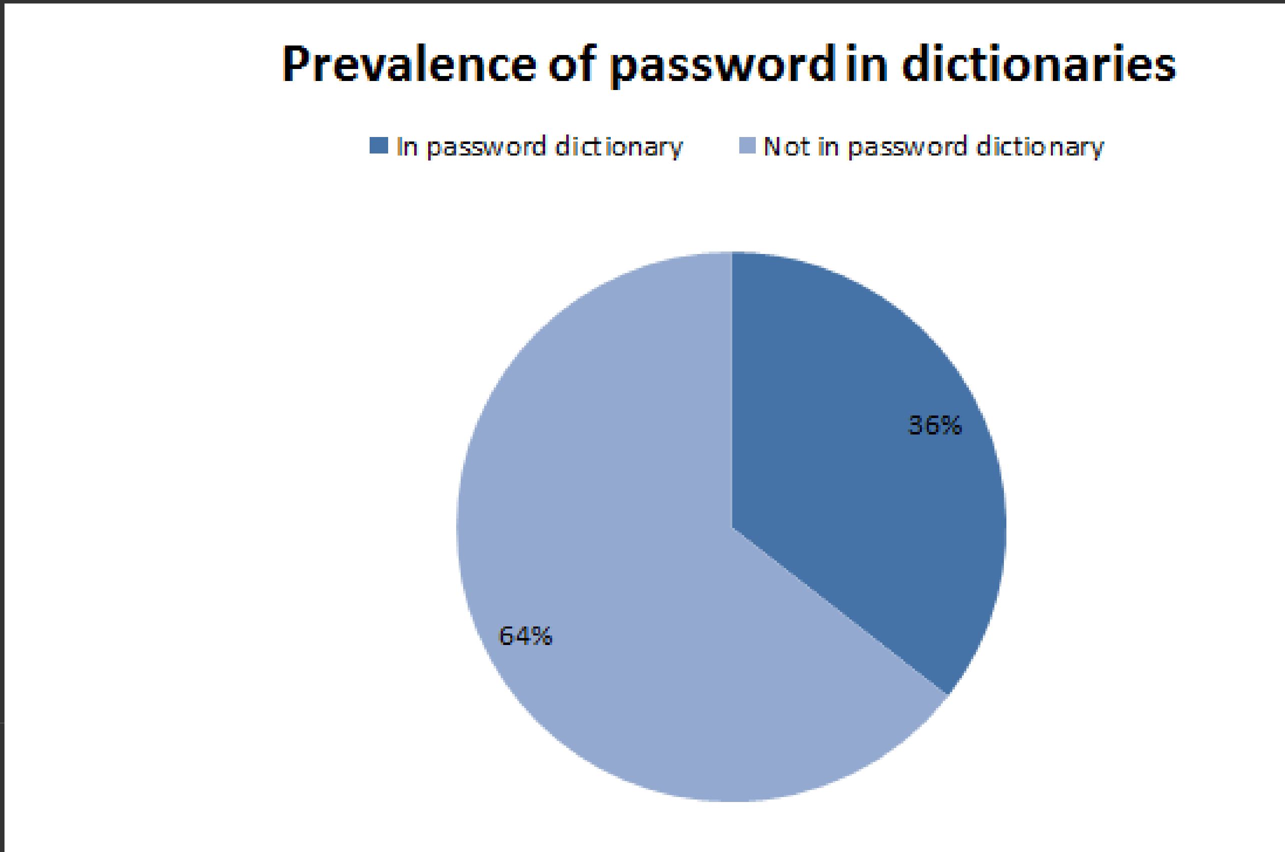


Character Type Exclusivity

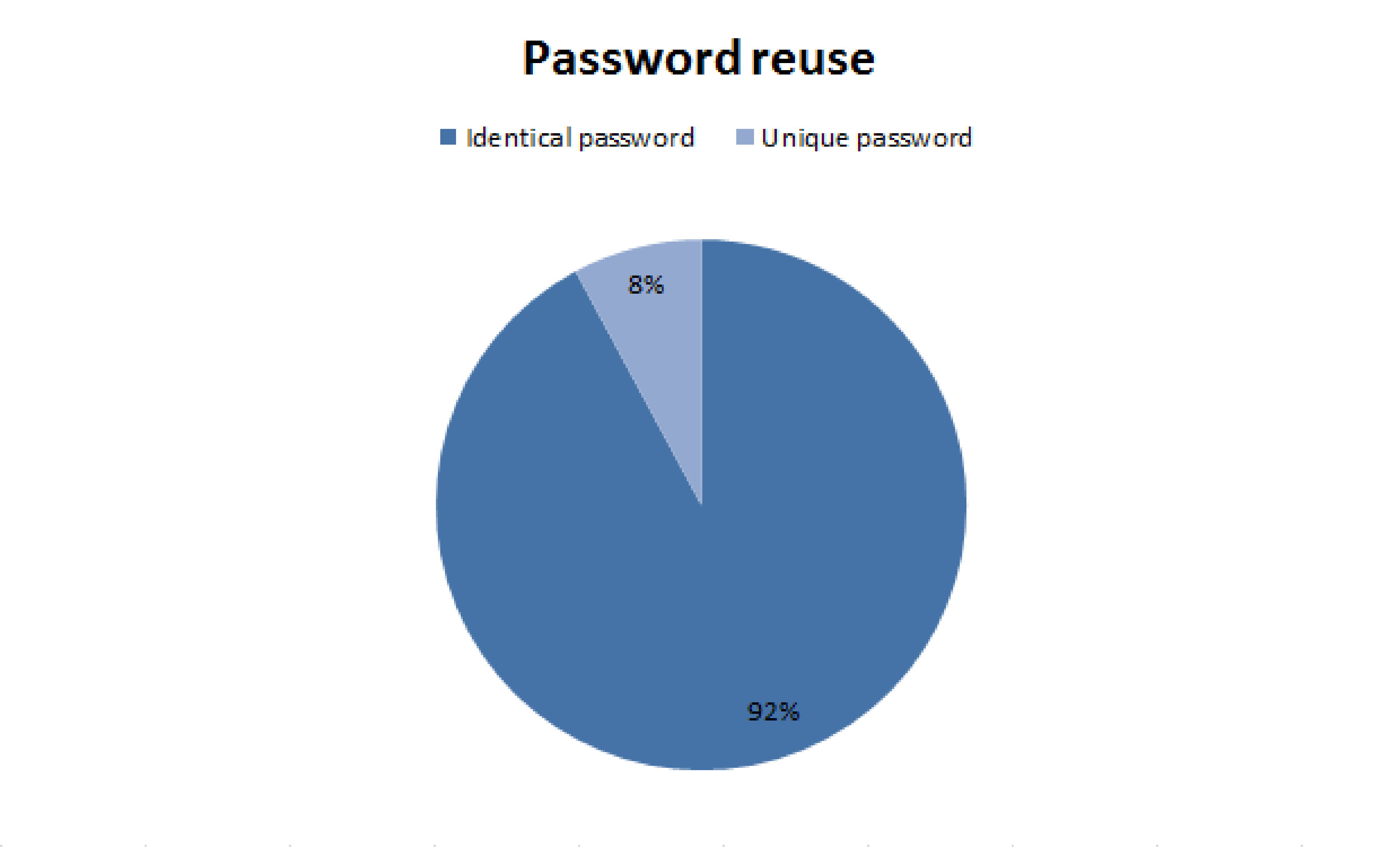


Randomness

- Top 25 passwords
  - *seinfeld, password, winner, 123456, purple, sweeps, contest, princess, maggie, 9452, peanut, shadow, ginger, michael, buster, sunshine, tigger, cookie, george, summer, taylor, bosco, abc123, ashley, bailey*



Uniqueness (across Sony)



Summary

- Not surprising but alarming
- Passwords too short, simple, predictable, shared across systems
  - Generally < 10 characters
  - Only using alphanumeric
  - Generally shared

Who is LulzSec?

- *For 50 days until it disbanded, the group's unique blend of humour, taunting and unapologetic data theft made it notorious. (June 2011)*
- Extracts from Interview with "Sabu"
  - http://www.newscientist.com/article/dn20649-exclusive-first-interview-with-key-lulzsec-hacker.html?full=true

LulzSec Hacks Timeline

Despite adopting a gentlemanly character from the popular Rage Comics as their mascot, incorporating the Nyan Cat meme into their exploits, and claiming a motive of "doing it for the lulz," the Lulz Security hacker collective has no allegiance to Anonymous.

May 7th: "X Factor"

The Target: Upcoming US version of talent and variety show The X Factor.

The Damage: LulzSec published the names, birthdates, phone numbers, and email addresses of an estimated 250,000 contestants.

Grade

Good execution
Boring Target

B

May 10: Fox.com

Impressive

LulzSec Hacks Timeline

Despite adopting a gentlemanly character from the popular Rage Comics as their mascot, incorporating the Nyan Cat meme into their exploits, and claiming a motive of "doing it for the lulz," the Lulz Security hacker collective has no allegiance to Anonymous.

May 7th: "X Factor"

The Target: Upcoming US version of talent and variety show The X Factor.

The Damage: LulzSec published the names, birthdates, phone numbers, and email addresses of an estimated 250,000 contestants.

Grade

Good execution
Boring Target

B

May 10: Fox.com

Impressive

May 10: Fox.com

The Target: Fox.com

The Damage: Fox.com's internal site configuration was revealed, along with a database of 407 sales contacts including their names, email addresses, passwords, and other senitive data.

Impressive targeting of sales contacts for maximum damage

A

May 15th: UK ATMs

The Target: UK ATM Database

The "Damage": LulzSec published a database of 3134 ATMs in the UK, including their ID #s, the companies that owned them, their locations, the machine type, and how much each charges.

what do you expect to do with this?

F

May 23rd: Sony Music Japan

The Target: Sony Music Japan

The Damage: A small and unimportant snippet of Sony Japan's internal data was published.

Embarassing breach of security, but little damage.

C

May 30th: PBS

The Target: PBS

The Damage: Main site defaced with Nyan Cat, false article about Tupac still being alive published to look like PBS, entire DNS map and server configuartion revealed, and databases of staffers, authors, and pressroom leaked.

Hilarious, stylish, and well-executed.

A

June 2nd: "Sownage"

LulzSec begins naming their operations and issuing press

Absolutely Devastating

June 2nd: "Sownage"

LulzSec begins naming their operations and issuing press releases.

The Target: SonyPictures International and Sony BMG

The Damage: LulzSec published user databases for various promotions and properties including AutoTrader, Restles Beauty, Del Boca Vista Sweepstakes, and private partner and admin data.

Absolutely Devastating

A

June 3rd: "Fuck FBI Friday"

The Target: FBI Affiliates Infraguard and Unveillance. Also Nintendo for some reason.

The Damage: The emails addresses, user names, and passwords of 180 clients of FBI accredited security firm Infraguard were comprimised, in addition to the name and home address of Unveillance CEO Karim Hijazi, and webserver configuration data for Nintendo.com.

Poorly Represented. No damgage done to actual FBI.

B

June 6th: "Sownage Part 2"

The Target: Sony Computer Entertainment Developer Network

The Damage: Scedev.net source code and Sony BMG internel network map published.

Well-executed, but damage is difficult to assess.

C

June 10th: Pron.com

The Target: Registered users of pornography site Pron.com

More entertaining than most hacks.

June 10th: Pron.com

The Target: Registered users of pornography site Pron.com

The Damage: Over 26,000 email addresses and passwords were leaked, including those belonging to a handful of government and military personnel.

More entertaining than most hacks.

A

June 13th: Titanic Takeover Tuesday

The Target: The United States Senate. Also video game company Bethesda Softworks

The "Damage": LulzSec published so-called "internal data" from a webserver used only for PUBLIC USE. Although the act garnered much press attention, nothing of any value was comprimised.

The only impressive part was the press generated, but the hack was crap.

F

June 14th: Various DDoS Attacks

The Targets: EVE Online, League Of Legends, The Escapist, and Minecraft servers.

The Damage: Lots of gamers were unable to play their favorite games.

DDoS attacks are not hacking. I love Minecraft. Your guys suck!

F

June 15th: Hack Request Line Open

The Targets: Lulzsec begins taking requests.

CIA.gov DDoSed
LulzSec openly mocks 4chan.
Factions of Anonymous begin to attack LulzSec-related sites.

Challenging Anonymous? You have my full attention.

How it was done

- Mainly through
  - SQL Injection
  - Cross Site Scripting
  - Remote Server Includes (Seldom used by other hackers)

Who is “Sabu”

- I'm a man who believes in human rights and exposing abuse and corruption. I generally care about people and their situations. I'm into politics and I try my best to stay on top of current events.

We've seen you cast as everything from the greatest of heroes to the most evil of villains.

- **How would you characterise yourself?**

- It is hard for me to see myself as either. I am not trying to be a martyr. I'm not some cape-wearing hero, nor am I some supervillain trying to bring down the good guys. I'm just doing what I know how to do, and that is counter abuse.

How did you get involved with Anonymous?

- When I found out about what happened to Julian Assange, his arrest in the UK and so on, I found it absolutely absurd. So I got involved with Anonymous at that point.

What would you say to people think Antisec/ Anonymous/LulzSec are just troublemakers?

- Would you rather your millions of emails, passwords, dox [personal information] and credit cards be exposed to the wild to be used by nefarious dealers of private information? Or would you rather have someone expose the hole and tell you your data was exploitable and that it's time to change your passwords? I'm sure we are seen as evil for exposing Sony and others, but at the end of the day, we motivated a giant to upgrade its security.

But what about hacks that were done "for lulz"?

- Yes, some hacks under LulzSec were done for the lulz, but there are lessons learned from them all. In 50 days, you saw how big and small companies were handling their user data incorrectly. You saw the US federal government vulnerable to security issues that could have just as easily been exploited by foreign governments. You saw affiliates of the US government handling sensitive emails and they themselves ignored the FBI's better practice manuals about password re-use.

So what would an Antisec "win" look like?

- There is no win. There's just change and education.

Are you afraid of being caught?

- There is no fear in my heart. I've passed the point of no return. I only hope that if I am stopped, the movement continues on the right path without me

He was caught … and turned

- Sabu was arrested on 7 June 2011
  - Hector Xavier Monsegur, age 28, single father of two
- Began assisting the FBI secretly
- Gave evidence to FBI which resulted in Anonymous and Lulz members being arrested
- March 2012 identity leaked and he declared a snitch
- Pleaded guilty to a slew of crimes
- He then started working for the US Government
- Feb 2013 he should have been sentenced but mysteriously was not …
- May 2014 let off with time served:7 months

Arrests

- Anonymous
  - 3 arrested in Spain (Barcelona, Valencia & Almeria), all in their 30’s
  - 32 in Turkey (police raids across 12 provinces)
    - 9 were minors and have been released
  - 6 arrested in the UK
    - 5 in Jan and 1 in April
    - Three teenagers (15,16,19) others in 20’s
    - Amazon, the Bank of America, Mastercard, PayPal and Visa's website in December 2010
  - USA issued 40 warrants for arrest in Feb 2011
- LulzSec
  - 21 June 2011 – 19 year old Ryan Cleary arrested in Essex – LulzSec claim he isnt part of them, just an assistant

The game continues...

- The authorities keep investigating
- The hackers keep hacking

The game continues ...

- Mid July 2011
  - Lulz comes out of retirement to hack Rupert Murdoch’s servers
    - Took down all News International’s DNS Servers
    - Redirected UK Sun tabloid readers to fake news story proclaiming Murdoch’s death
    - After Sun IT regained control, hacked again to redirect to Lulz Twitter account
  - Tweets
    - “We had joy, we had fun, we have messed up Murdoch’s Sun”
    - For all you new people that are watching us right now: This is what we do, how we do it. High-quality entertainment for you”

The game continues ...

- FBI Arrests more “anonymous” members
  - NPR Article : “FBI Tries to Send Message with Hacker arrests”
  - “We want to send a message that chaos on the internet is unacceptable, [even if] hackers can be believed to have social causes, it’s entirely unacceptable to break into websites and commit unlawful acts.”

The game continues ...

- Lulz & Anonymous issue a statement
  - Hello thar FBI and international authorities
  - The statements made seem to be directed at Anonymous and Lulz, we are happy to provide a response
  - Let us be clear here, Mr Chabinsky, you may find breaking into websites unacceptable, here is what we find unacceptable
    - Governments lying to their citizens and inducing fear and terror to keep them in control by dismantling their freedom bit by bit
    - Corporations aiding and conspiring with governments while taking billions for federal contracts they can’t fulfil
    - Lobby conglomerates who push own agenda for higher profits, deeply involved in government to corrupt and keep status quo
    - These governments and corporations are our enemy we will continue to fight them through all methods including hacking and exposing lies

The game continues

- Lulz/Anonymous statement continued...
  - We are not scared, your arrests are meaningless as you cannot arrest an idea, and attempting to do so will make your citizens angry until they roar in one gigantic choir
  - Let me ask you good sir, when was the internet not the Wild Wild West? Do you really believe you were in control of it at any point? You were not.
  - That does not mean everyone behaves like an outlaw. You see, most people do no behave like bandits if they have no reason to
  - We have become bandits on the internet because you have forced our hand.
  - The Anonymous bitchslap rings through your ears like hacktivism movements of the 90s
  - We're back – and we're not going anywhere. Expect us.

The game continues ...

- More?
  - Italian police hacked 25/7/2011
    - Cybercrime division CNAIPIC hacked
    - 8 Gig of data taken
    - Internal documents
    - External parties : Exxon Mobil, US Dept of Agriculture, Australian Ministry of Defence
    - Management structures, pictures of CNAIPIC staff
    - Part of #AntiSec movement, revenge for arrests
  - Austrian TV license feel collection authority 22/7/2011
    - 214,000 files
    - 96,000 contain sensitive bank information
    - GIS has started informing customers about lost data
    - Done by AustrAnon, linked to Anonymous

The game continues ...

- More?
  - 28/7/11 More than 500mb of NATO data leaked
  - 29/7/11 Info from FBI contractor ManTech and emails from Department of Homeland Security leaked
  - 30/7/11 Info on Miss Scotland contestants posted from The Sun
  - 6/8/11 10Gig of data from 76 rural US Sheriffs offices leaked online in retaliation for arrests last month
  - 7/8/11 Personal info of 45000 police officers in Ecuador after Ecuador government threatens Anonymous
  - 14/8/11 BART is hacked and info of users (names, passwords, personal info – why stored in cleartext??) retaliation for comms shutdown
  - 17/8/11 BART police officer details (names, home addresses, email addresses, passwords) released in further retaliation

The game continues...

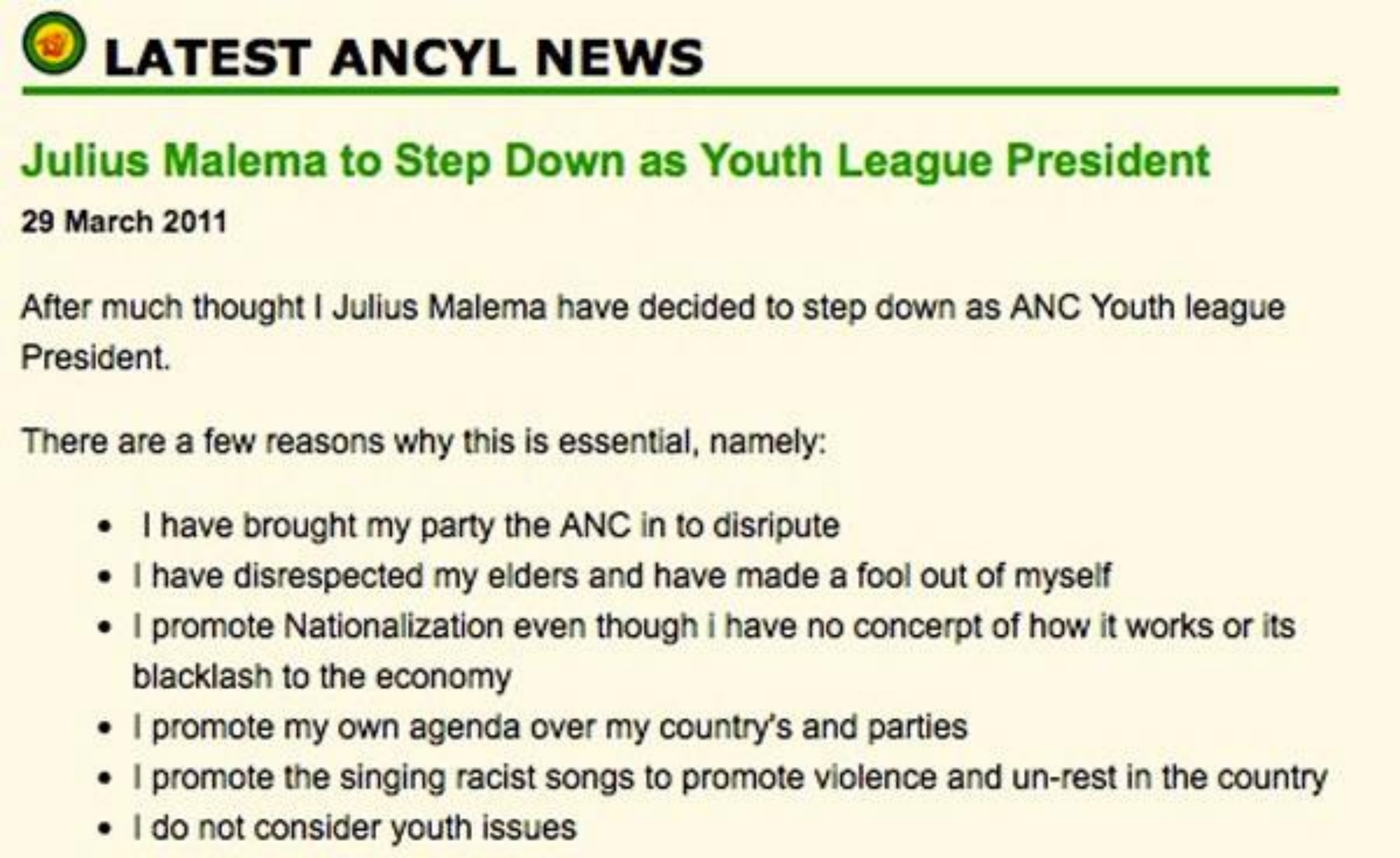
- The authorities keep investigating
- The hackers keep hacking

- Will it ever stop?
  - The wave may slow but the hackers will never stop

The ANC YL

Again and again 2011

First – March 2011



LATEST ANCYL NEWS

Julius Malema to Step Down as Youth League President

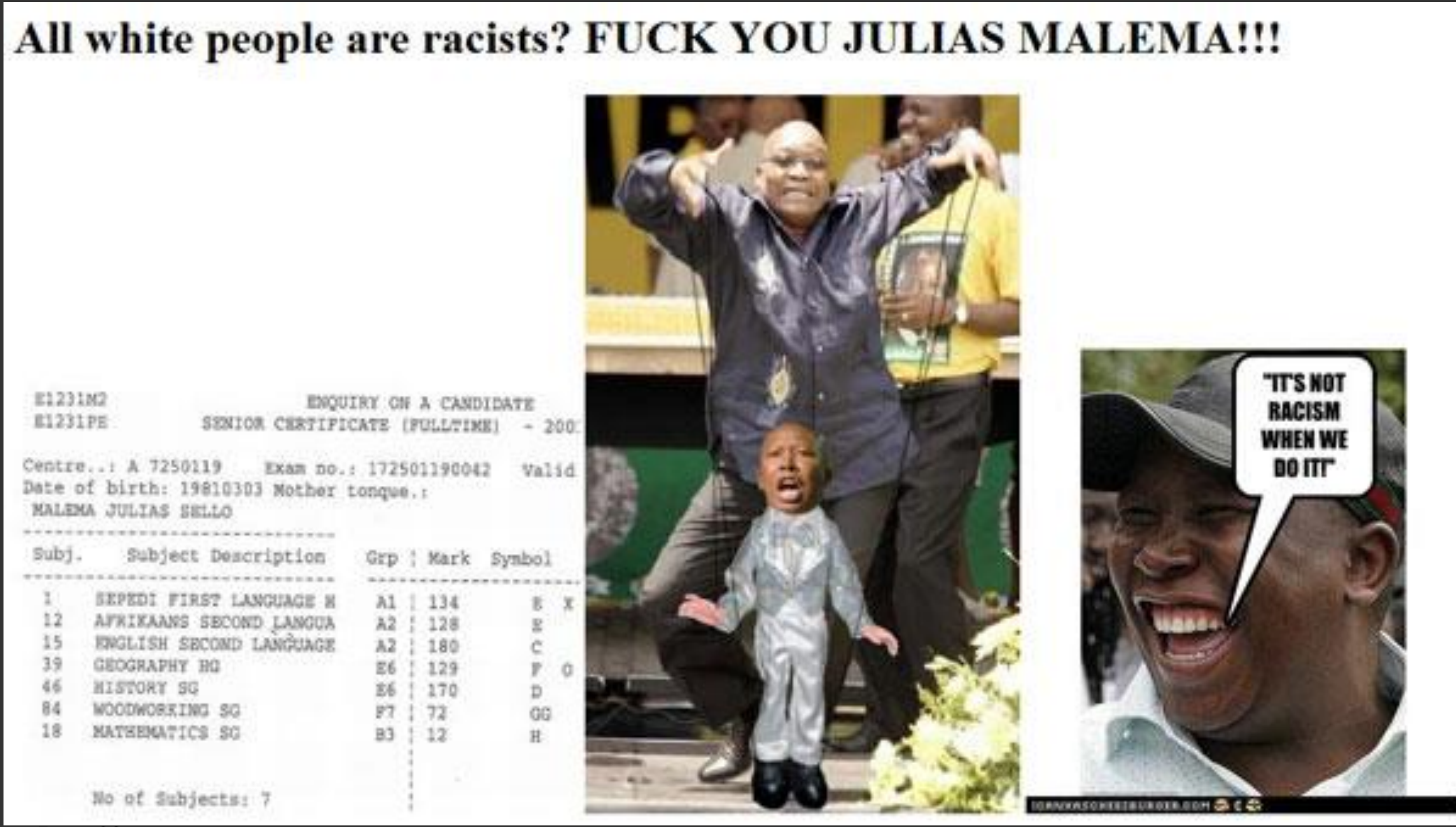
29 March 2011

After much thought I Julius Malema have decided to step down as ANC Youth league President.

There are a few reasons why this is essential, namely:

- I have brought my party the ANC in to disripute
- I have disrespected my elders and have made a fool out of myself
- I promote Nationalization even though i have no concerpt of how it works or its blacklash to the economy
- I promote my own agenda over my country's and parties
- I promote the singing racist songs to promote violence and un-rest in the country
- I do not consider youth issues

Second – May 2011

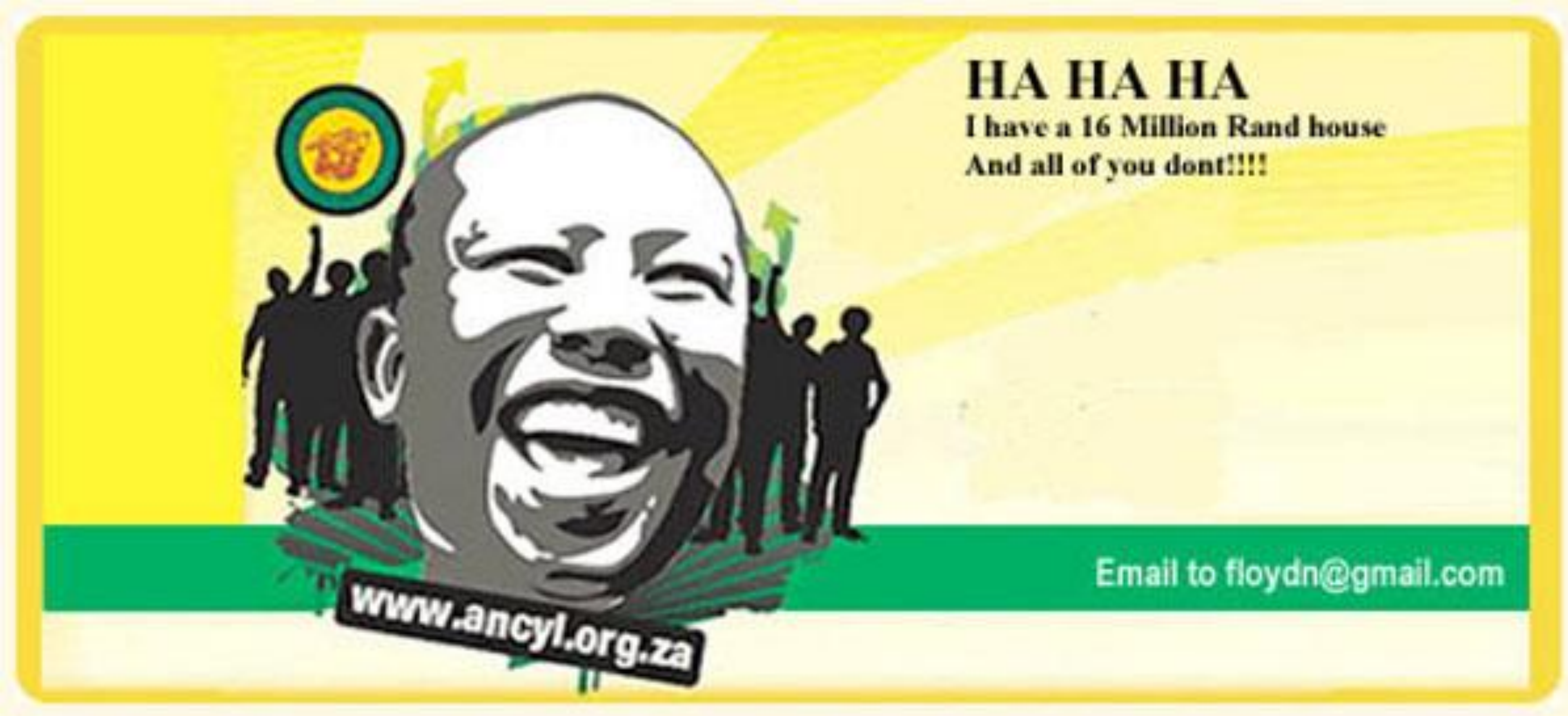


All white people are racists? FUCK YOU JULIAS MALEMA!!!

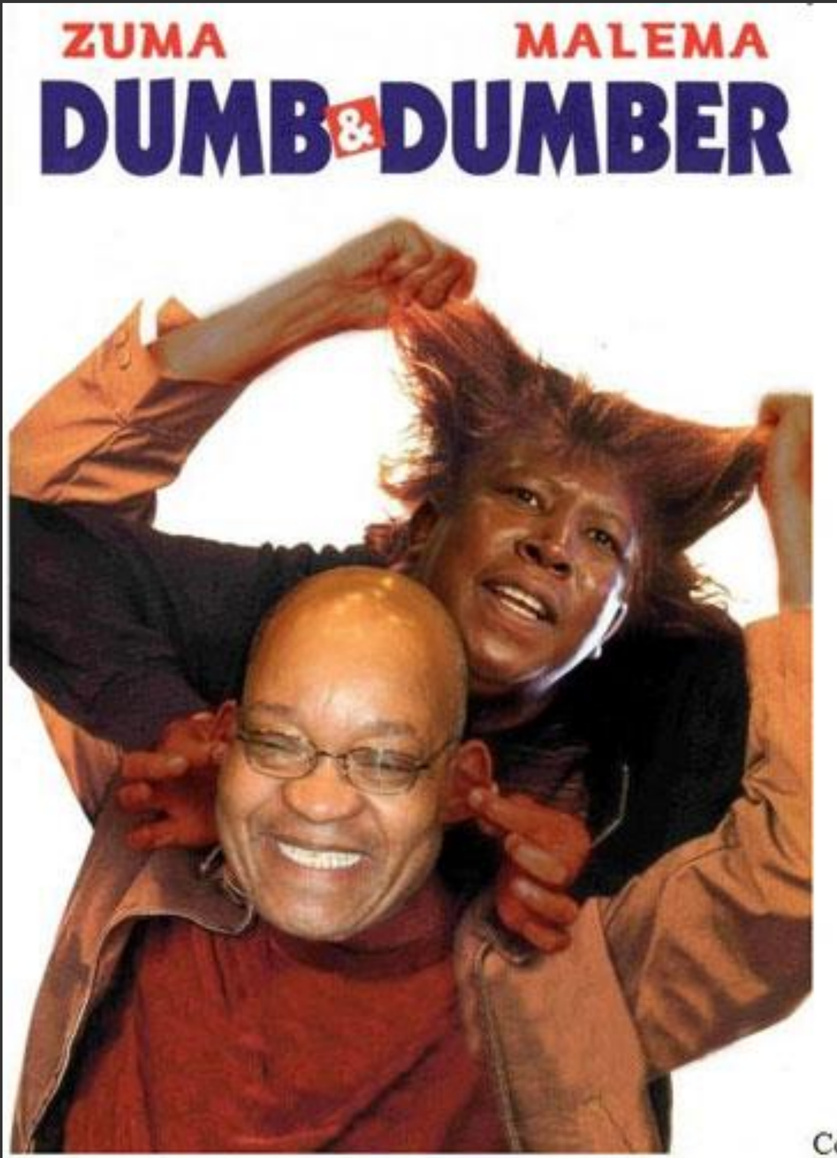
```
E1231M2                     ENQUIRY ON A CANDIDATE
E1231PE           SENIOR CERTIFICATE (FULLTIME)  - 200

Centre..: A 7250119    Exam no.: 172501190042   Valid
Date of birth: 19810303 Mother tonque.:
 MALEMA JULIAS SELLO
-----------------------------
 Subj.    Subject Description    Grp ¦ Mark  Symbol
-----------------------------    --------------------
  1    SEPEDI FIRST LANGUAGE H    A1 ¦ 134        E  X
 12    AFRIKAANS SECOND LANGUA    A2 ¦ 128        E
 15    ENGLISH SECOND LANGUAGE    A2 ¦ 180        C
 39    GEOGRAPHY HG               E6 ¦ 129        F  O
 46    HISTORY SG                 E6 ¦ 170        D
 84    WOODWORKING SG             F7 ¦ 72         GG
 18    MATHEMATICS SG             B3 ¦ 12         H
                                     ¦
       No of Subjects: 7             ¦
```

Third – 24 July 2011



Fourth – 26 July 2011



Computer science is NOT on his matric results!

Fifth – 26 August 2011

“You will see my conrades (sic) nothing will happen to me. I Dare the ANC, Jacob Zuma, Hawks, Public Protector or the Police to come after me. “I will bury you”

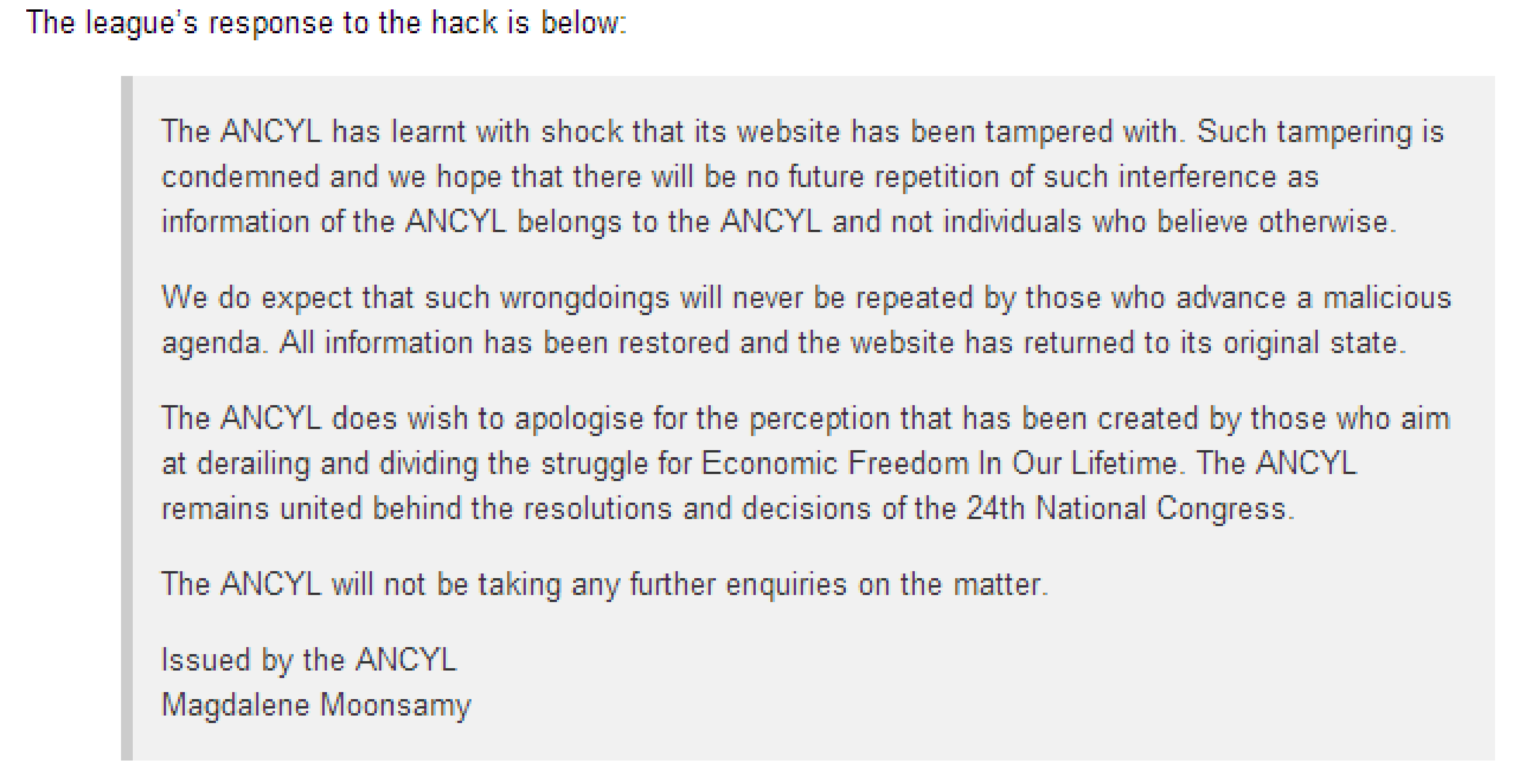
“Letter of the President of the ANCYL”.

But an irate league ANCYL spokesman Floyd Shivambu rejected it as fake.

“We’ve been hacked before, but this time it’s really bad. We are determined that this time the police must catch the hackers. We must put a stop to this kind of thing,” said Shivambu.

Sixth– 2 May 2012

- Julius’ name was removed from the ANCYL website
- The president position just had “blank” next to it



The league's response to the hack is below:

> The ANCYL has learnt with shock that its website has been tampered with. Such tampering is condemned and we hope that there will be no future repetition of such interference as information of the ANCYL belongs to the ANCYL and not individuals who believe otherwise.
>
> We do expect that such wrongdoings will never be repeated by those who advance a malicious agenda. All information has been restored and the website has returned to its original state.
>
> The ANCYL does wish to apologise for the perception that has been created by those who aim at derailing and dividing the struggle for Economic Freedom In Our Lifetime. The ANCYL remains united behind the resolutions and decisions of the 24th National Congress.
>
> The ANCYL will not be taking any further enquiries on the matter.
>
> Issued by the ANCYL
> Magdalene Moonsamy

Who got hacked in 2012

- Postbank (South Africa)
  - January 2012
  - R42 million stolen
    - Accounts opened in December
    - Accessed computer of employee in Rustenburg Post Office
    - Withdrawals from ATM’s across the country in a 3 day sting
  - Cybercrime syndicate
  - The Hawks Successfully tracked down some of the gang
  - One man sentenced to 15 years in jail
  - Recovered some of the money
- Linkedin hacked
  - June 2012
  - 161 million users
  - 6 million accounts password hashes disclosed (unsalted)
  - Unclear how many were actually
  - At first they didn’t know how it was done and took >7 hours to acknowledge

Who got hacked in 2012 part 2

- eHarmony (dating site)
  - June 2012 1.5 million password hashes stolen
  - System unknowingly converted user passwords to upper case
  - eHarmony played it down, saying is only a small fraction of its users
- Drop Box (again) August 2013
  - Usernames and passwords stolen from LinkedIn, eHarmony and Last.fm used to access Dropbox accounts
  - Stolen password accessed Dropbox employee account
  - Dropbox denied for few days before coming clean
- South Carolina Social Security records
  - October 2012
  - 3.6 million social security records, 78% of population of state
  - Included 670 000 businesses
  - 3 weeks to come to light, after being reported to US Secret Service
- Nationwide Mutual
  - December 2012
  - 1.1 million records : names, social security numbers, date of birth, employers name, gender, marital status
  - Hackers thought to be outside of the USA

Who got hacked in 2013

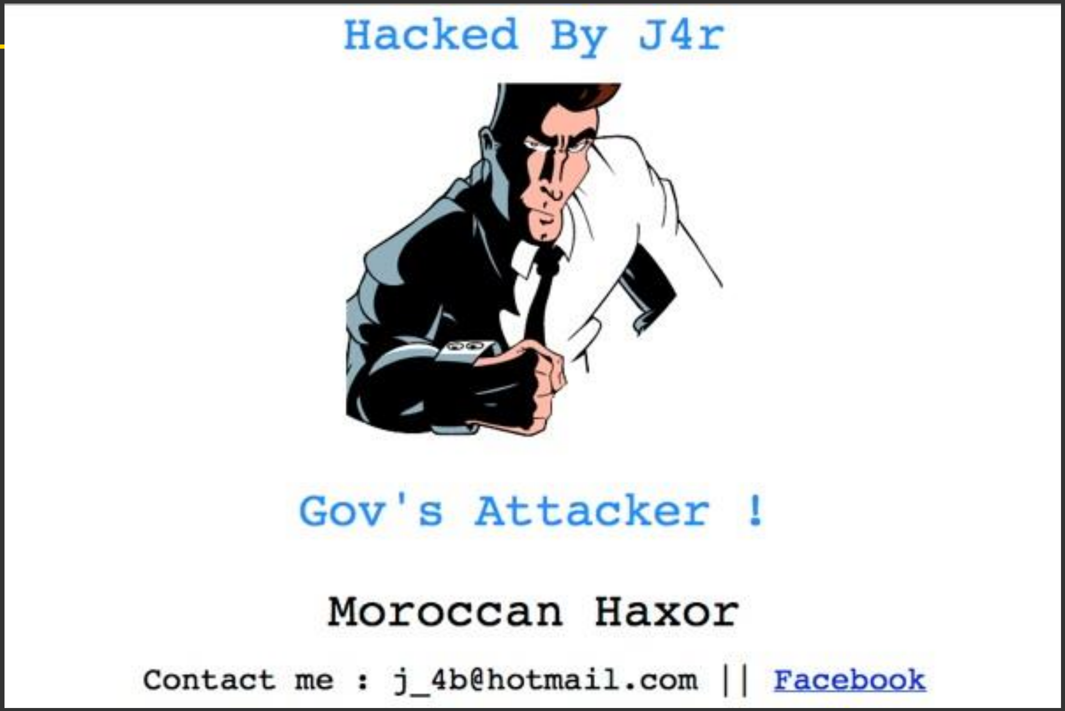
- South African Police Services
  - Press briefing 22/5/2013 – No confidential information leaked
  - Corporate systems hosted in Pretoria CBD, Website hosted by SITA
  - Lt General Ngubane : Info hackers got was all public
- However
  - When challenged on clearly private information leaked?
  - SITA general manager Daniel Mashao admitted it was an oversight
  - Should have changed the system to be more secure
  - Should have encrypted the data
- “What concerns us is that there are cases where people provided information [on potential crimes],”

Who got hacked in 2013

- South African Police Services
  - @DomainerAnon was the hacker
  - A simple SQL injection attack was all that was needed, poor web design
  - Back in late 2012 I tweeted the fact that I believed the SAP servers were vulnerable to attack
  - The attack on the SAPS website on Friday (17 May 2013) was in retaliation for “the lack of adequate justice for the slaughtered miners” at Marikana.
  - Highlighted fact that SAP’s own duty of care, security of information on its servers is questionable
  - Domainer wasn’t worried about being caught by the SAPS
  - despite Ngubane stating that an investigation by Crime Intelligence Division had already yielded some results
  - “Crime Intelligence?” Domainer quipped. “Sorry I had to laugh. They have nothing… just pretending that they are doing their job.”

Who got hacked in 2014

- Public Investment Corporation
  - 17 August 2014



Hacked By J4r

Gov's Attacker !

Moroccan Haxor

Contact me : j_4b@hotmail.com || Facebook

- Heartbleed
  - April 2014

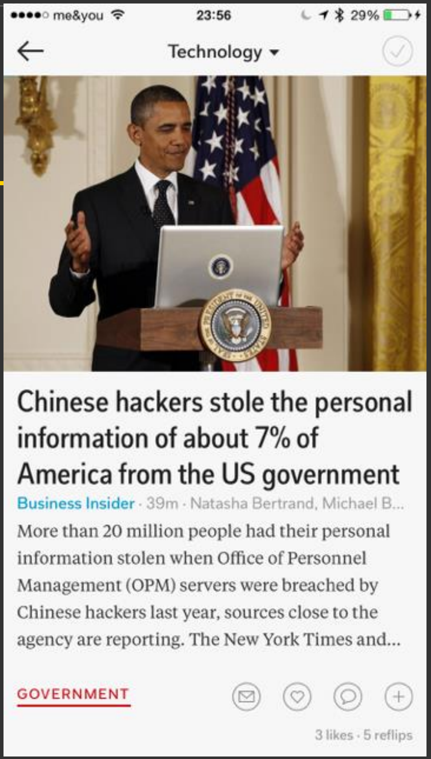
- Everyone?
  - Russian Hacking Group
  - Used Botnets (CyberVor)
  - Identified & hacked 400 000 websites
  - Over 4.5 billion records
  - Stole over 1.2 billion unique email addresses & passwords
    - http://www.bbc.com/news/technology-28654613

Heartbleed? Who was affected?

All of us

- Servers (600 000 of them)
  - Yahoo, Imgur, Flickr
  - Eventbrite, mail.com, indiegogo
  - Lonelyplanet, Kaspersky, Rapidshare
  - Creativecommons.org, bidorbuy.co.za
  - DigitalRiver, Barclaycardus, utorrent.com
- Devices
  - Lots

Who got hacked in 2015



Chinese hackers stole the personal information of about 7% of America from the US government

Business Insider · 39m · Natasha Bertrand, Michael B...

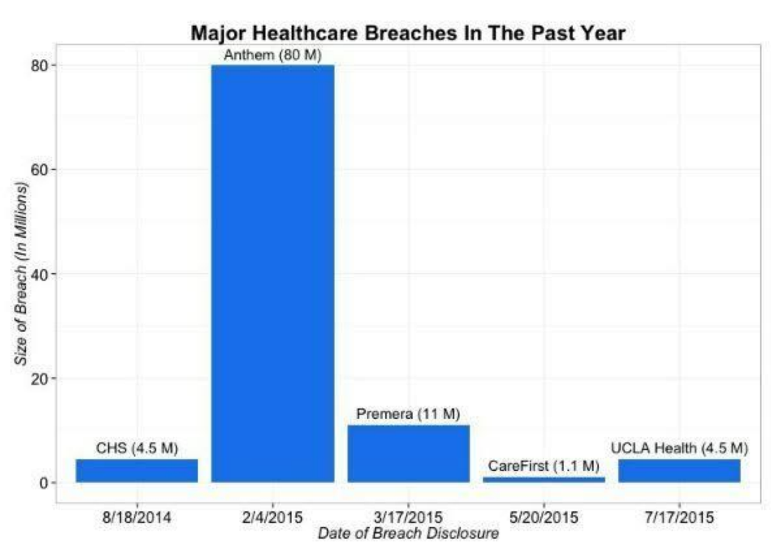
More than 20 million people had their personal information stolen when Office of Personnel Management (OPM) servers were breached by Chinese hackers last year, sources close to the agency are reporting. The New York Times and...

GOVERNMENT

3 likes · 5 reflips

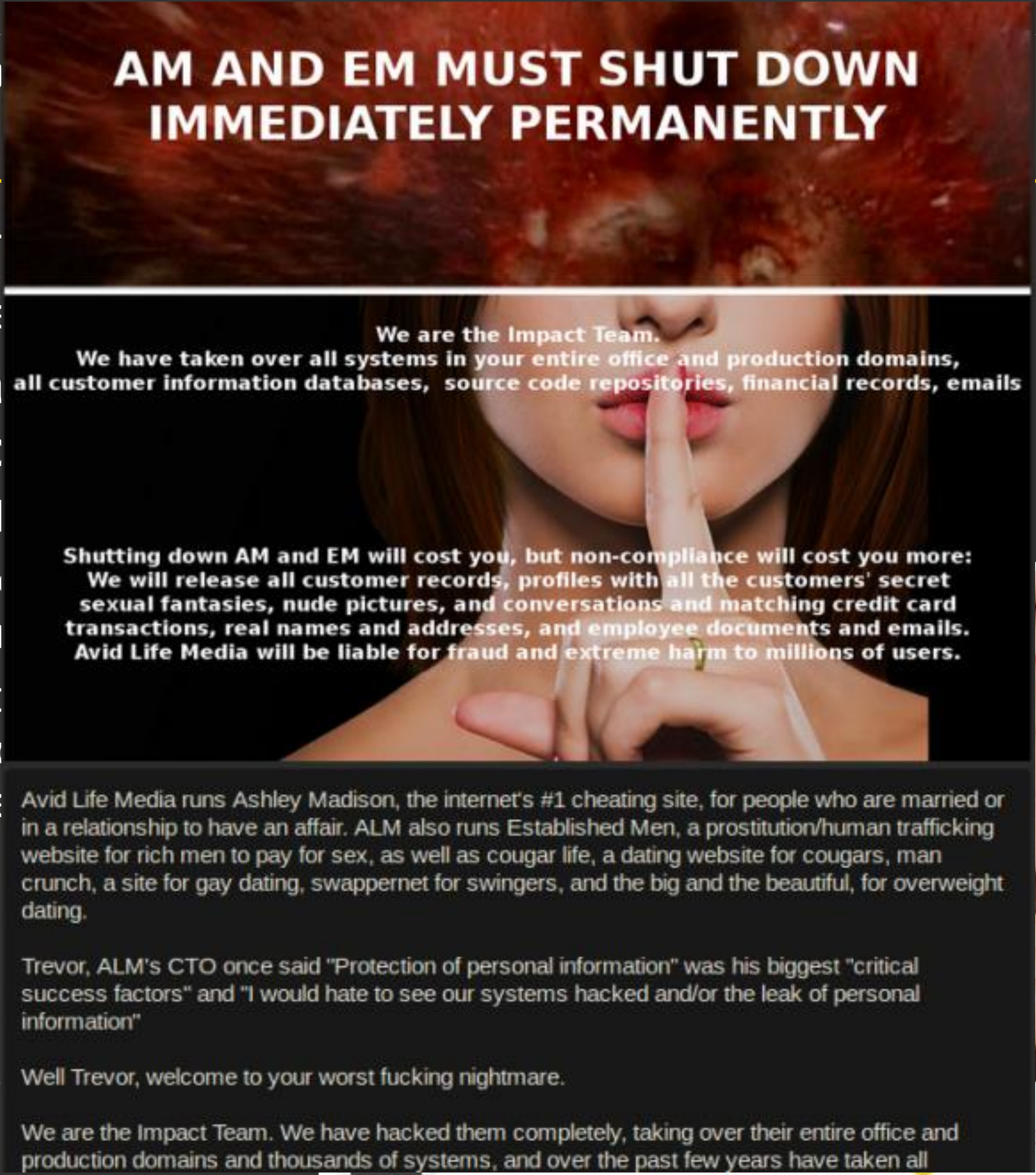
- USA Office of Personnel Management (OPM)
  - Chinese hackers stole personal information
  - 21.5+ million people, 7% of all Americans
  - Security Clearance information
  - Biometric Information
  - We have a problem,
    please reset your fingerprints!

- Healthcare Breaches
  - Anthem 4 Feb 2015 80M
  - Premera 17 March 2015 11M
  - CareFirst 1.1M 20 May 2015
  - UCLA Health 4.5M   17 July 2015



Who go

- AdultFrier
  - 3.9m use
- AshleyMa
  - Online C
  - Charged
  - Purchas name an
  - “Too bac They’re and dese discretio



AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY

We are the Impact Team.
We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails

Shutting down AM and EM will cost you, but non-compliance will cost you more: We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails. Avid Life Media will be liable for fraud and extreme harm to millions of users.

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

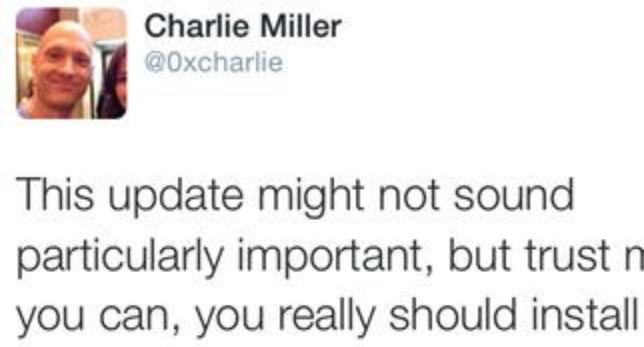
Who got hacked in 2015

- Video Jeep

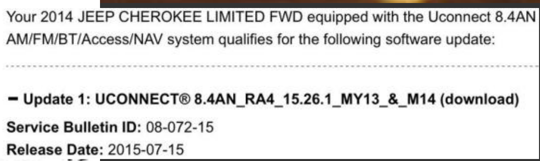
Who got hacked in 2015

- Cars? Yes Cars
  - Jeep Grand Cherokee
  - Cherokee SUV
  - Dodge Ram Pickups
  - Many others (1.4m+)

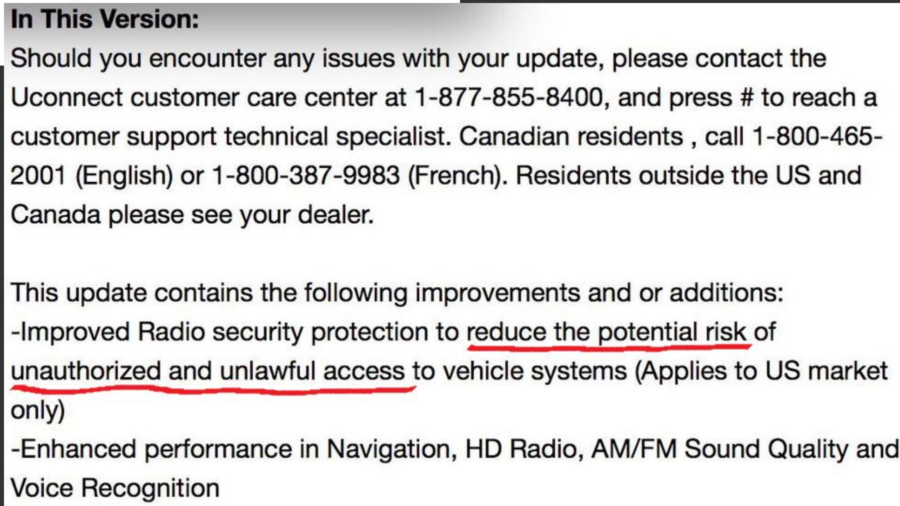
- Via in-car entertainment system
  - Apply a “patch” to your car via a USB dongle
- What does the hack allow?
  - Remote access via cellular connection
  - Scan for make model IP location
  - Brakes, Transmission, Steering


Charlie Miller
@0xcharlie

This update might not sound particularly important, but trust me, if you can, you really should install this one.


Your 2014 JEEP CHEROKEE LIMITED FWD equipped with the Uconnect 8.4AN AM/FM/BT/Access/NAV system qualifies for the following software update:

– Update 1: UCONNECT® 8.4AN_RA4_15.26.1_MY13_&_M14 (download)
Service Bulletin ID: 08-072-15
Release Date: 2015-07-15


In This Version:
Should you encounter any issues with your update, please contact the Uconnect customer care center at 1-877-855-8400, and press # to reach a customer support technical specialist. Canadian residents , call 1-800-465-2001 (English) or 1-800-387-9983 (French). Residents outside the US and Canada please see your dealer.

This update contains the following improvements and or additions:
-Improved Radio security protection to reduce the potential risk of unauthorized and unlawful access to vehicle systems (Applies to US market only)
-Enhanced performance in Navigation, HD Radio, AM/FM Sound Quality and Voice Recognition

Who got hacked in 2015

- Video Tracking Point

Hacking Guns!

- $13000 TrackingPoint rifle with assisted tracking scope
- Running Linux
- Accessible via Wi-Fi (default password)
- Manipulate critical settings or disable it
- No indication of tampering
- Can be permanently altered

Who got hacked in 2015

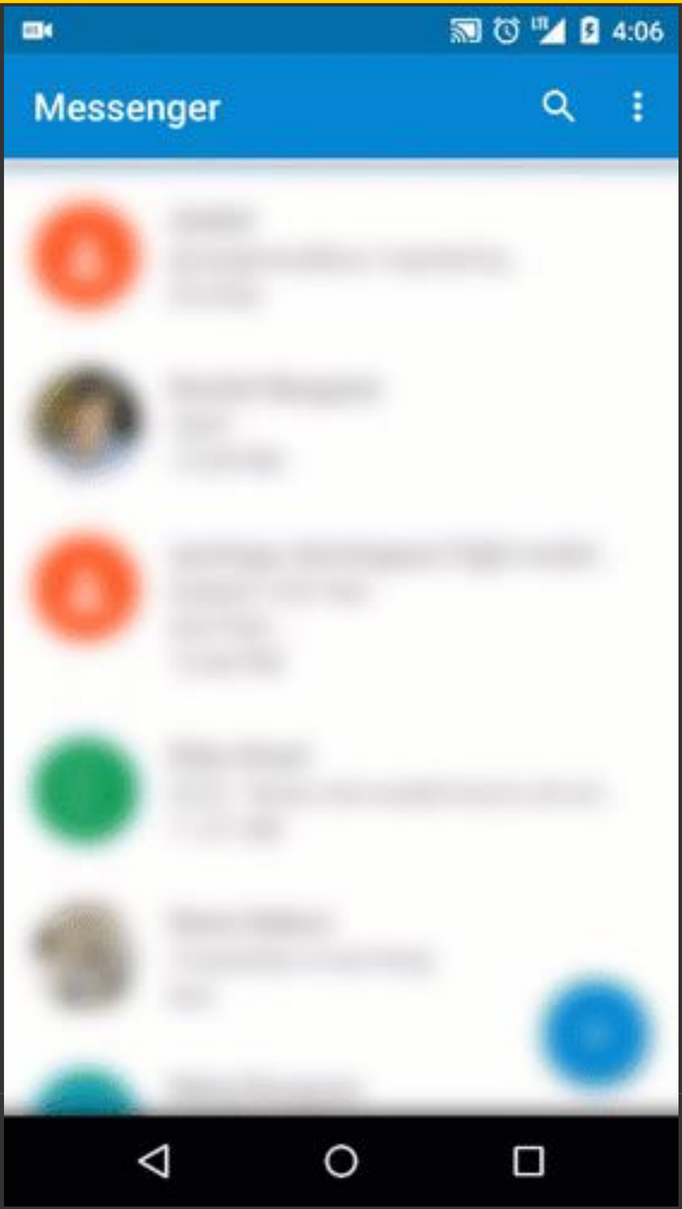
- Stagefright
  - 2015’s very own Heartbleed
  - All Android phone users??
  - Nearly a billion phones are vulnerable!

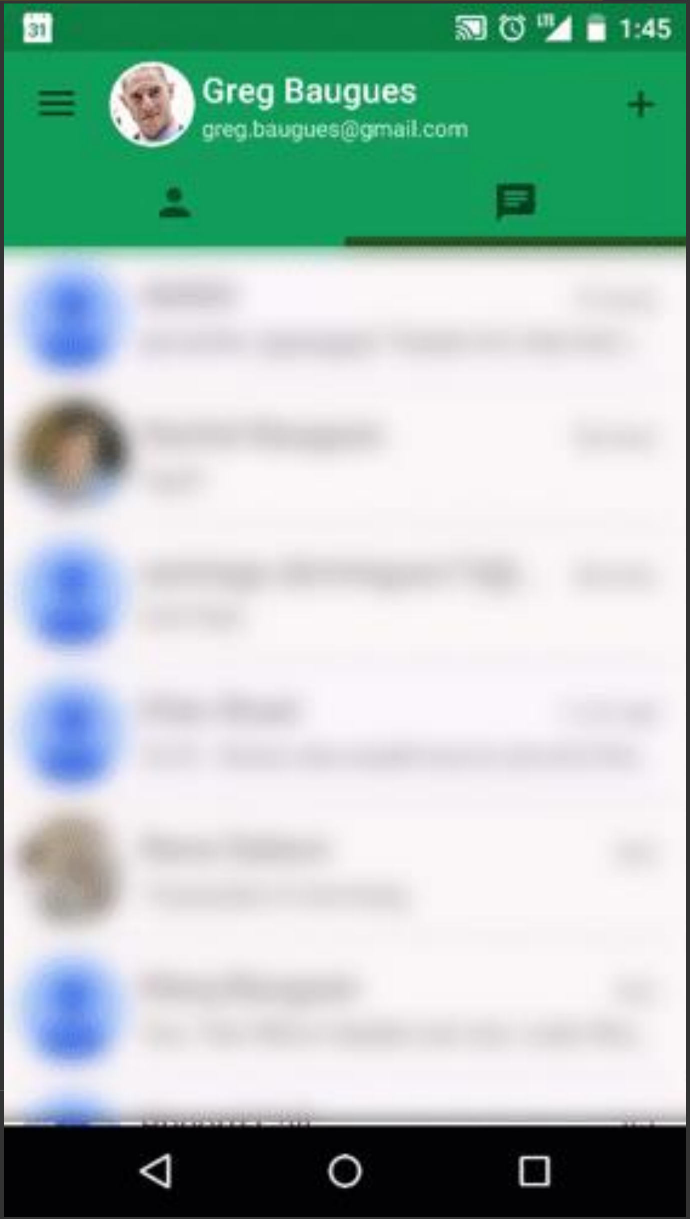
- How?
  - Just a single MMS
  - And you don’t even need to open it to be affected
  - You may not even hear the message received notification

- As of 30 July 2015 was not yet patched
- You must turn off the auto media downloading

Check your phone now

- Disable auto downloading of media files via MMS?





Spy vs Spy : The Snowden Files

Who is watching you?

- USA
- United Kingdom
- France
- China
- India
- New Zealand
- Australia
- Israel
- Germany

Who else??

Spy vs Spy : USA

StuxNet

- The official start of the Cyberwar?
- Signed off by Obama or started under Bush?
- Joint effort by USA & Israel : targeted Iranian nuclear prog

PRISM

- Info leaked by Edward Snowden
- Confirmation of what suspected : Massive snooping

X-KeyScore

- designed to collect against entire global telecomms network
- all digital communications
- Realtime “big data” analysis

Spy vs Spy : United Kingdom

- Member of the Five Eyes electronic eavesdropping alliance
- USA paid UK Spy Agency (GCHQ) 100 million pounds over 3 years
- 7,000% increase in personal data available to GCHQ over five years
- GCHQ wants to 'exploit any phone, anywhere, anytime
- Tapped more than 200 global fibre optic cables (operation Tempora)
- 10 gigabits of data per second (entire British library 192x / day)
- Phone calls, email messages, Facebook entries & access to websites
- Handling 600 million “telephone events” per day
- 550+ analysts from UK & USA sifting data
- 850 000 NSA employees and contractors can access the data

"As a general rule, so long as you have any choice at all, you should never route through or peer with the UK under any circumstances“ Edward Snowden, NSA whistleblower

Spy vs Spy : USA’s Five Eye Partners

- Agencies have connected parts of their top-secret and secret networks to allow for communication
- Jointly banned Lenovo computers since 2006 (reported, then denied)
- Banned ZTE & Huawei on spying concerns (US House of representatives Oct 2012)

“International efforts are coordinated by the NSA's Foreign Affairs Directorate (FAD). The FAD has full cooperation with its so-called "Five Eye partners" in the UK, Australia, New Zealand, and Canada, and these agencies are even better or worse (depending on your viewpoint) at collecting data. Typically, these countries practice "full take" scooping every bit of data and storing it for later perusal. “ Snowden

Spy vs Spy : China

- Nine in 10 APT tools made in China (FireEye : Infosec 2013)
- China behind 96% of cyber espionage campaigns seen in the last year (Verizon 2013)
- 19% of breaches linked to Chinese government and aimed to steal intellectual property (Verizon 2013)
- APT1 (codename) working for People’s Liberation Army and other Chinese APT teams tracked by Mandiant for over a decade
- Backdoors in Chinese tech : ZTE, Huawei

Spy vs Spy : France

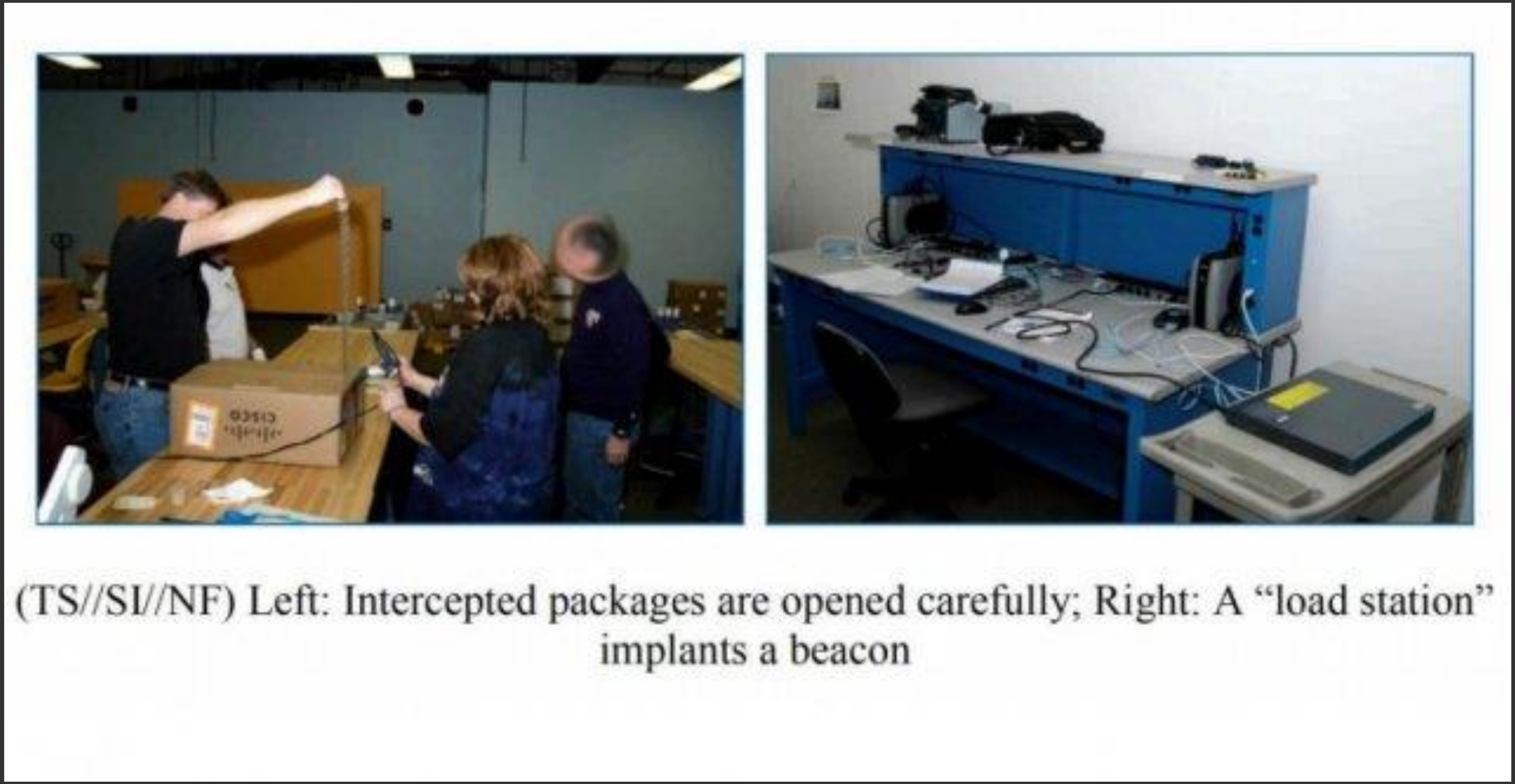
- Vast surveillance programme similar to Prism
- Spied on French public
- emails, text messages, phone records, accessing of Facebook and Twitter, and internet activity
- Intercepted signals from computers and phones in France as well as between France and other countries
- Secret, "outside any serious control" and illegal
- Probably the biggest information centre in Europe after the English

Spy vs Spy

Just who can you trust?

Spy vs Spy

Not the US Government : NSA intercepts and backdoors Cisco Routers

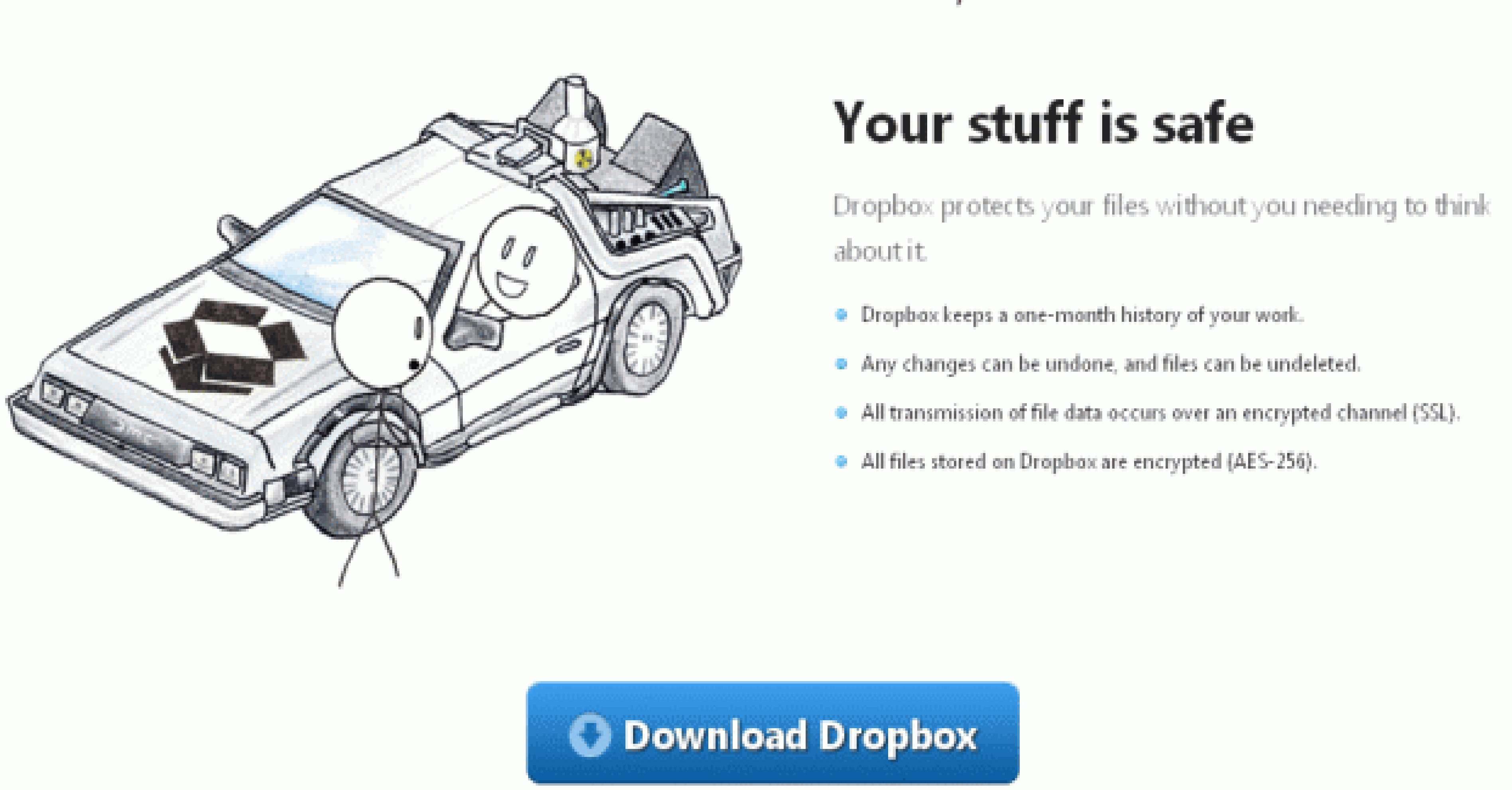


(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Maybe Switzerland?

- 300 year strong reputation for Swiss bank accounts
- Not part of the EU
- Strong privacy and data protection legislation
- Privacy culture
- Access to data requires Swiss court order proving guilt or liability

Dropbox lied to customers?



Your stuff is safe

Dropbox protects your files without you needing to think about it.

- Dropbox keeps a one-month history of your work.
- Any changes can be undone, and files can be undeleted.
- All transmission of file data occurs over an encrypted channel (SSL).
- All files stored on Dropbox are encrypted (AES-256).

The allegations

- Soghoian alleges Dropbox falsely claimed :
  - Your files are AES256 encrypted
  - Even our employees can’t access your files

- Dropbox responds
  - “We believe this complaint is without merit, and raises old issues that were addressed in our blog post on April 21, 2011,” company spokeswoman Julie Supan

However

- On the 13th April Dropbox changed their website :
  - “All files stored on Dropbox servers are encrypted (AES256) and are inaccessible without your account password” to
  - “All files stored on Dropbox servers are encrypted (AES 256)”
- And
  - “Dropbox employees aren’t able to access user files, and when troubleshooting an account, they only have access to file metadata (filenames, file sizes, etc. not the file contents).” to
  - “Dropbox employees are prohibited from viewing the content of files you store in your Dropboxaccount, and are only permitted to view file metadata (e.g., file names and locations).”
- Why the big deal about this?
  - users at risk of government searches, rogue Dropbox employees, and even companies trying to bring mass copyright-infringement suits

The question

How did OSAMA do it?

How Osama did it?

- No phone, no internet connection
- Typed up messages on a disconnected computer
- Save to flash disk
- Trusted courier to internet café
  - Send outgoing messages
  - Save incoming messages
- Drive back to Osama
- US Navy Seals seized roughly 100 flash memory drives when they killed bin Laden at his Abbottabad, Pakistan, compound a week and a half ago.
- Officials told the AP they “appear to archive the back-and-forth communication between bin Laden and his associates around the world.“

Source : TheRegister.co.uk

2 Case Studies

EFT System
End User Computing

Case Study : Electronic Funds Transfer

Why test ?

Hundreds of millions of rands of payments being made every year

Case Study : Electronic Funds Transfer

- **Scenario :**

  A multinational company approachedus to assess the security of their EFT infrastructure from the perspective of a malicious employee on the local network.

- **Objective :**

  Gain access to and process transactions on the EFT system.

Case Study : Electronic Funds Transfer

- **Champion :**

  The work was commissioned by senior management without the knowledge of IT

- **Purpose :**

  To gain understanding of the true current state and validate whether the position put forward by IT was a true reflection of reality

Case Study : Electronic Funds Transfer

- **Outcome :**
  - Gained full access to the mainframe based EFT application with supervisor and signatory privileges
  - This would have allowed us to fraudulently process transactions, alter account details and severely disrupt the company’s accounting system
  - Organisation failed test

Case Study : Electronic Funds Transfer

- **How It Was Done :**
  - Used company phone list to identify financial staff.
  - Obtained access to key workstations, allowing us to install key loggers, download sensitive data, obtained client software used to connect to EFT system.
  - Obtained access to the Windows NT domain allowing us to crack 98.8% of domain passwords.

Case Study : Electronic Funds Transfer

- **How It Was Done Continued :**
  - Accessed E-mail infrastructure with NT domain passwords. This allowed us to intercept sent email describing EFT signatories, limits etc.
  - Network eavesdropping allowed us to intercept all network traffic between the EFT system and workstations, including usernames & passwords.

Case Study : Electronic Funds Transfer

- **Results:**
  - Accessed the EFT system.
  - With the information obtained above it was trivial to log onto the EFT system as a privileged user and process transactions.
  - We were not detected.
  - The route we followed to achieve our objectives indicates the importance of a comprehensive security architecture.

Why test?

Determine the likelihood of and impact of the compromise of ***users*** *through use of non-technical means*

Case Study : End User Computing

- **Scenario :**

  A prominent financial services group approached us to perform a social engineering exercise to test the level of security awareness of their employees.

- **Objective :**

  To obtain unauthorized access to employees workstations/network access. Specifically senior management was targeted.

Case Study : End User Computing

- **Champion :**

  The work was commissioned by senior management of a business division, with the knowledge of IT executives.

- **Purpose :**

  To gain an understanding of the general level of security awareness within the organisation.

Case Study : End User Computing

- **Outcome :**
  - We were able to collect usernames and passwords from 9/10 employees targeted
  - Gained access to network and workstations of these key personnel (Secretary of director, Senior managers)
  - Organisation failed the test

Case Study : End User Computing

- **How It Was Done :**
  - Used company phone list to identify senior management staff and select targets
  - Used the switchboard to “spoof” and hide the origin of our calls. All our calls appeared to be from internal.

Case Study : End User Computing

- **How It Was Done Continued :**
  - Pretended a dangerous virus was present and all data could be lost
  - Informed user that automatic update had failed and updated must be done manually
  - Employees “panicked” and simply gave us their usernames and passwords.

Case Study : End User Computing

- **Results:**
  - 9 employees’ workstations and network access was compromised.
  - 1 employee was alert and did not compromise the organisation
  - Employees did not adhere to company policy.
  - The information obtained through social engineering could be used to further infiltrate the organisation.

Case Study : End User Computing

- **Other social engineering methods:**
  - Handing out memory sticks
  - Facebook / Linkedin / Twitter

Current observations and future predictions

Observations

- Attitude towards security is improving significantly
  - Appointment of security officers
  - Moving beyond policy, procedure and standards
    - More than just operating systems
    - Scorecards & dashboards
    - Big data and monitoring systems (Security Analytics)
    - Self assessment
    - Ongoing compliance testing
  - Protecting reputation and brand become a significant driver
- Privacy has been identified as requiring action
  - Protection of personal information act/bill
  - Will be enacted in March 2013, big implications
  - Still waiting August 2014…..

Biggest Issues for South African Companies

- Strategic
  - Privacy – Protection of Personal Information an Act shortly (Mar 2013)
  - Protection of reputation and brand
  - King 3 compliance
- Technical
  - Patch management
  - Secure Solution Selection and implementation
  - Complexity of environment (and trust)
  - User environment (Workstations) not secured
  - Data moving to the cloud
  - Skills, cost of skills and cost of technology solutions
  - Monitoring & Big Data
- Procedural
  - Ongoing compliance
  - Poor administrative practices
  - User Education

Watch what is going on

Monitoring attacks (26/11/2013-12/12/2013)

- Play Video

Monitoring attacks (24 hours Dec 2013)

Participating further

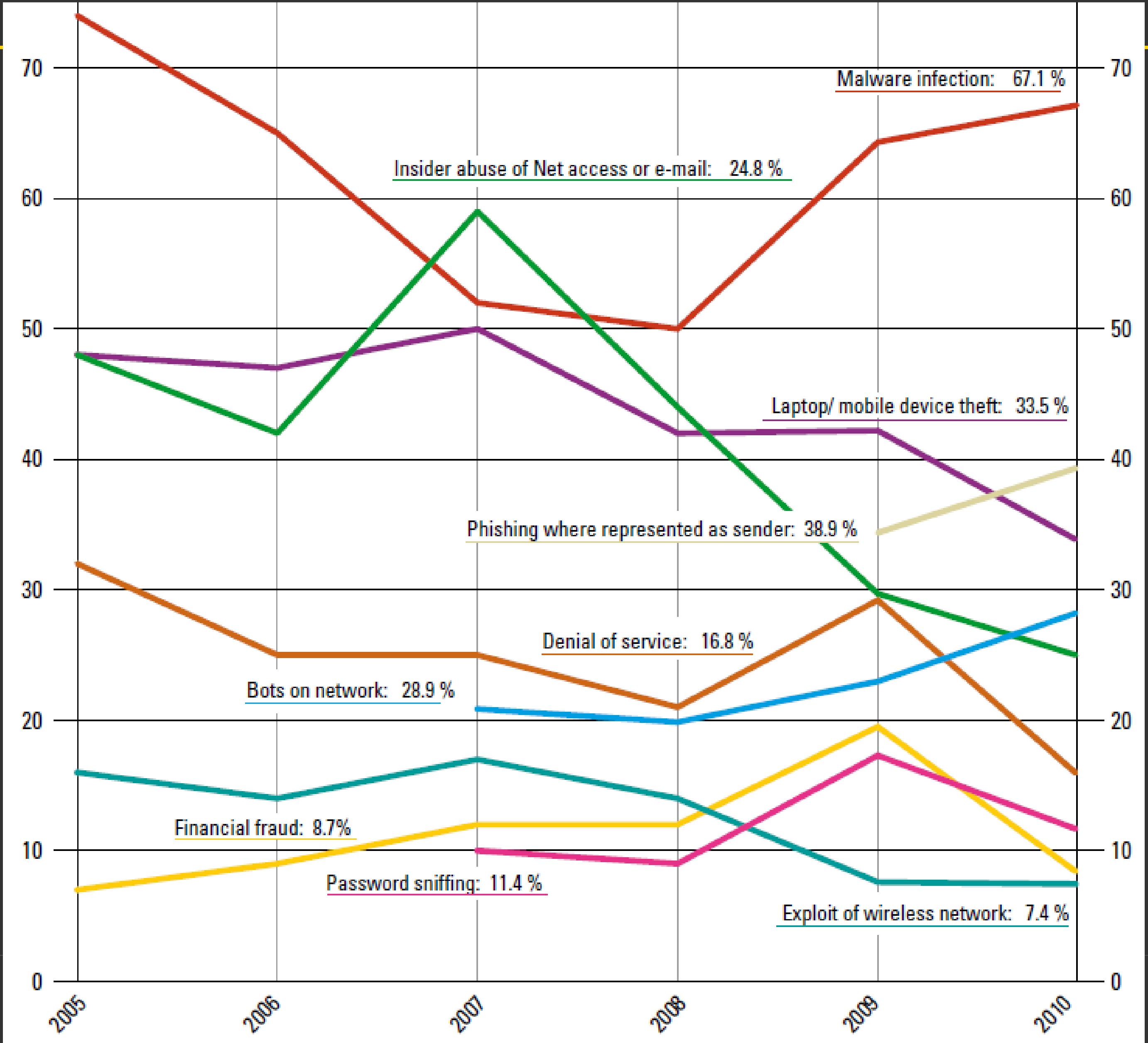
- ISACA KZN Chapter
  - WWW.ISACA.ORG.ZA
- ISG Africa / Whitehat
  - Regular meetings at UKZN : WWW.ISGAFRICA.ORG
- Institute of Internal Auditors – IT SIG
  - WWW.IIA.ORG.ZA
- Podcasts
  - WWW.DISCUSSIT.CO.ZA
- Follow me on twitter : jjza

Questions ??

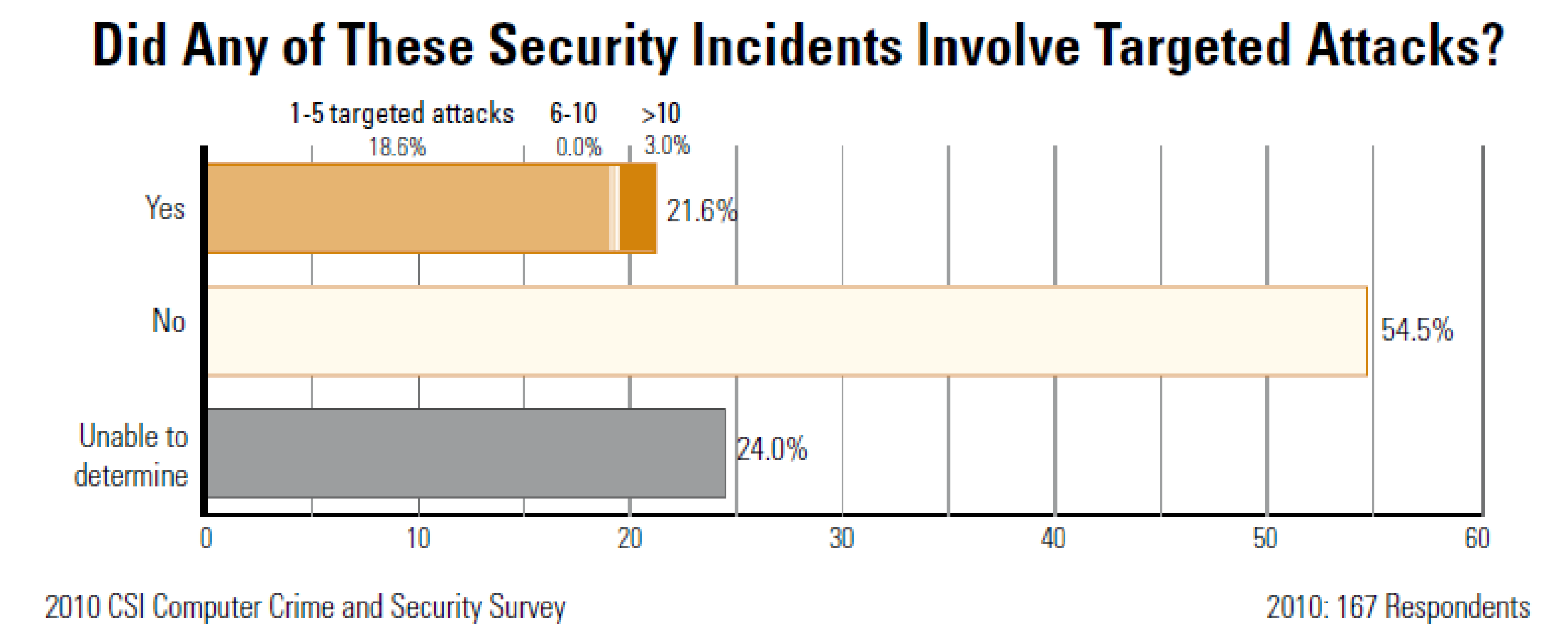
Contact :

Email :	justin.j.williams@gmail.com
Mobile :	082 772 9881
Website :	http://j-j.co.za
twitter	@jjza http://twitter.com/jjza
LinkedIn	Justin Williams, Durban, SA

CSI 2010 Survey : Types of attacks



CSI 2010/11 Survey : Targeting


Did Any of These Security Incidents Involve Targeted Attacks?
1-5 targeted attacks
>10
Yes
No
Unable to determine
2010 CSI Computer Crime and Security Survey
2010: 167 Respondents