Security & Ethics – 17 August 2012

UKZN MBA 2012

Justin Williams
Acting Head : Enterprise Information Security Management
Transnet

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

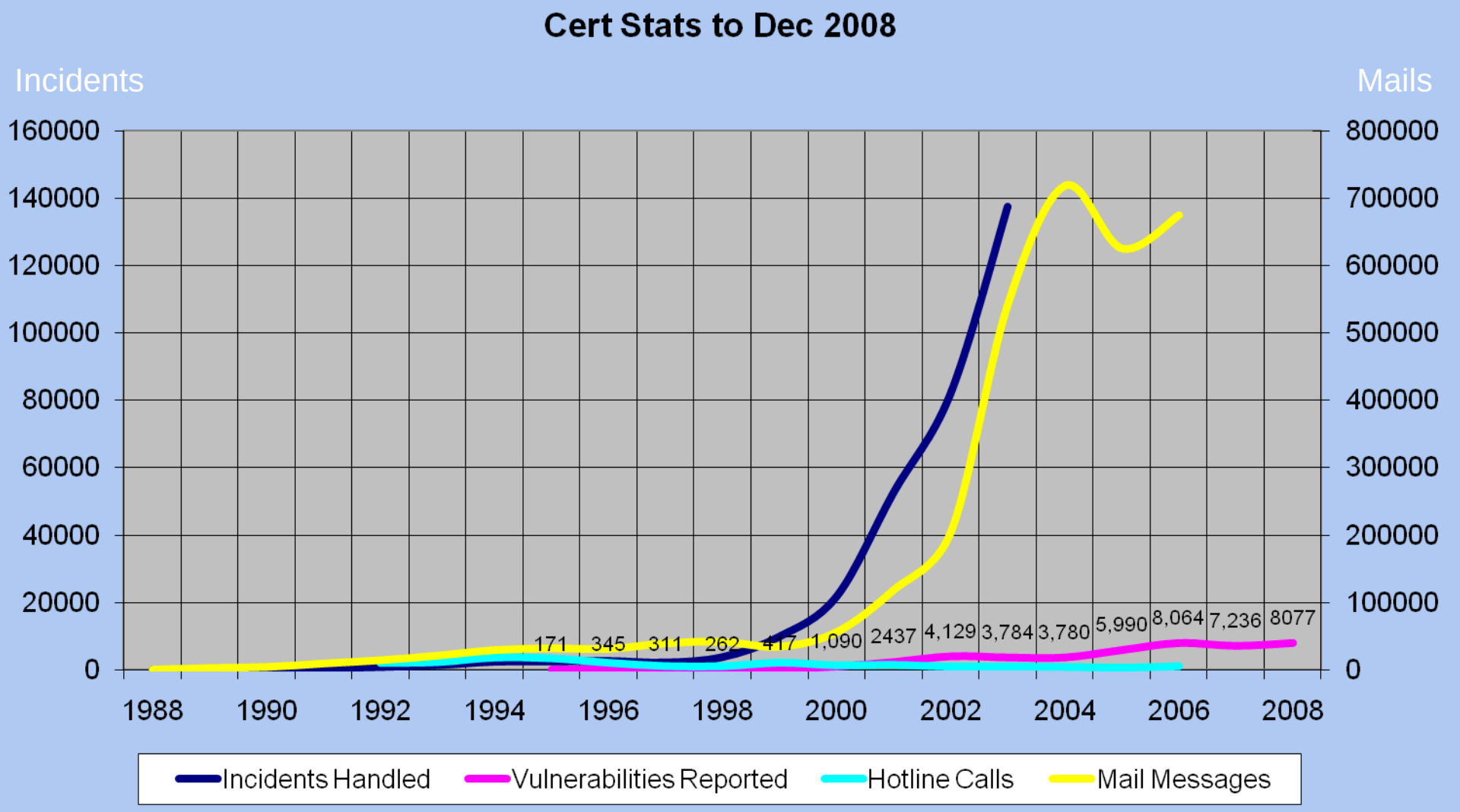
- Ethics are embodied in codes of professional conduct for IS professionals
  - Eg. Association of IT professionals (AITP), ISACA, ISC2
    - HTTP://WWW.ISACA.ORG.ZA
  - Recognises obligation to employer
    - Avoid conflicts of interest
    - Protect privacy & confidentiality etc
  - Also obligation 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



Selected “key” findings PWC 2011 survey

- Strategic trends in spending
  - Security is on the CFO “protect list”
  - Vulnerable to flavour of the year
  - Splash then diffusion
- Drivers aren’t new, but are trending at 4 year lows
- ***“Client requirements”*** are a more significant reason for infosec
- Largest increase in risk due to weaker partners and suppliers
- Some firms are allowing capabilities to degrade
- ISO reporting line moved away from CIO to business
- ***Social networks*** one of fastest growing areas of risk
- Mitigating consequences of breach through incident response now a leading priority

Drivers of infosec

Figure 1: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organisation. [1]

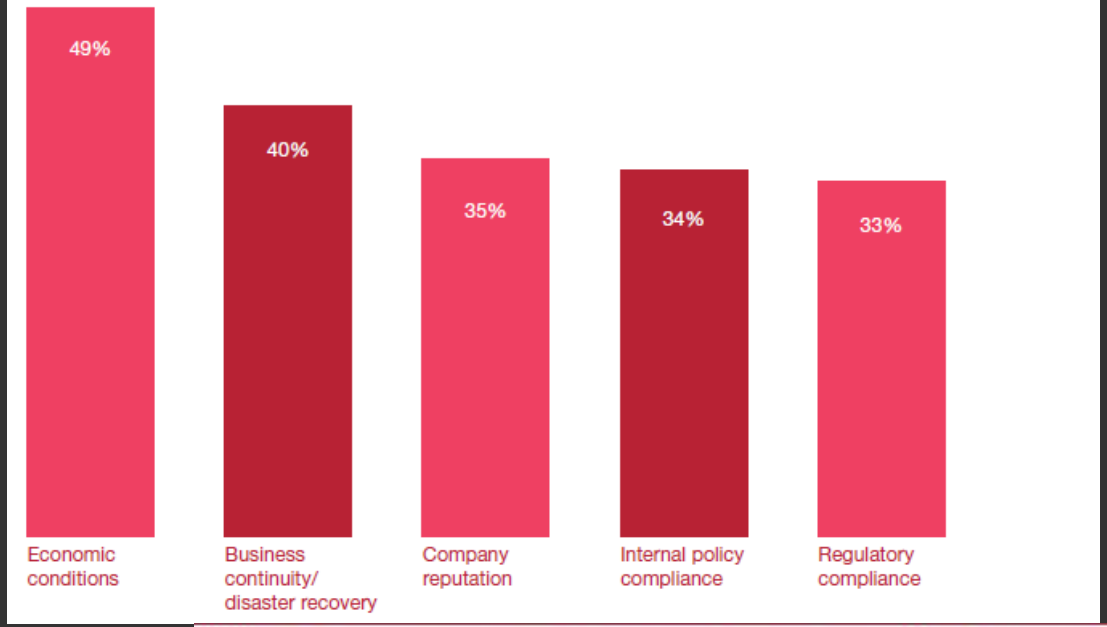


Figure 2: Percentage of respondents who identify the following business issues or factors as the most important drivers of information security spending in their organisation. [2]

	2007	2008	2009	2010	Three-year % change*
Economic conditions	n/a	n/a	39%	49%	n/a
Business continuity/disaster recovery	68%	57%	41%	40%	-41%
Company reputation	44%	39%	32%	35%	-20%
Internal policy compliance	51%	46%	38%	34%	-33%
Regulatory compliance	54%	44%	37%	33%	-39%

Justification of infosec

Figure 3: Percentage of respondents who identify the following factors when asked to reveal how information security is justified in their organisation. [3]

	2007	2008	2009	2010	Three-year % change*
Legal/regulatory environment	58%	47%	43%	43%	-26%
Client requirement	34%	31%	34%	41%	+21%
Professional judgment	45%	46%	40%	40%	-11%
Potential liability/exposure	49%	40%	37%	38%	-22%
Common industry practice	42%	37%	34%	38%	-10%
Risk reduction score	36%	31%	31%	30%	-17%
Potential revenue impact	30%	27%	26%	27%	-10%

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

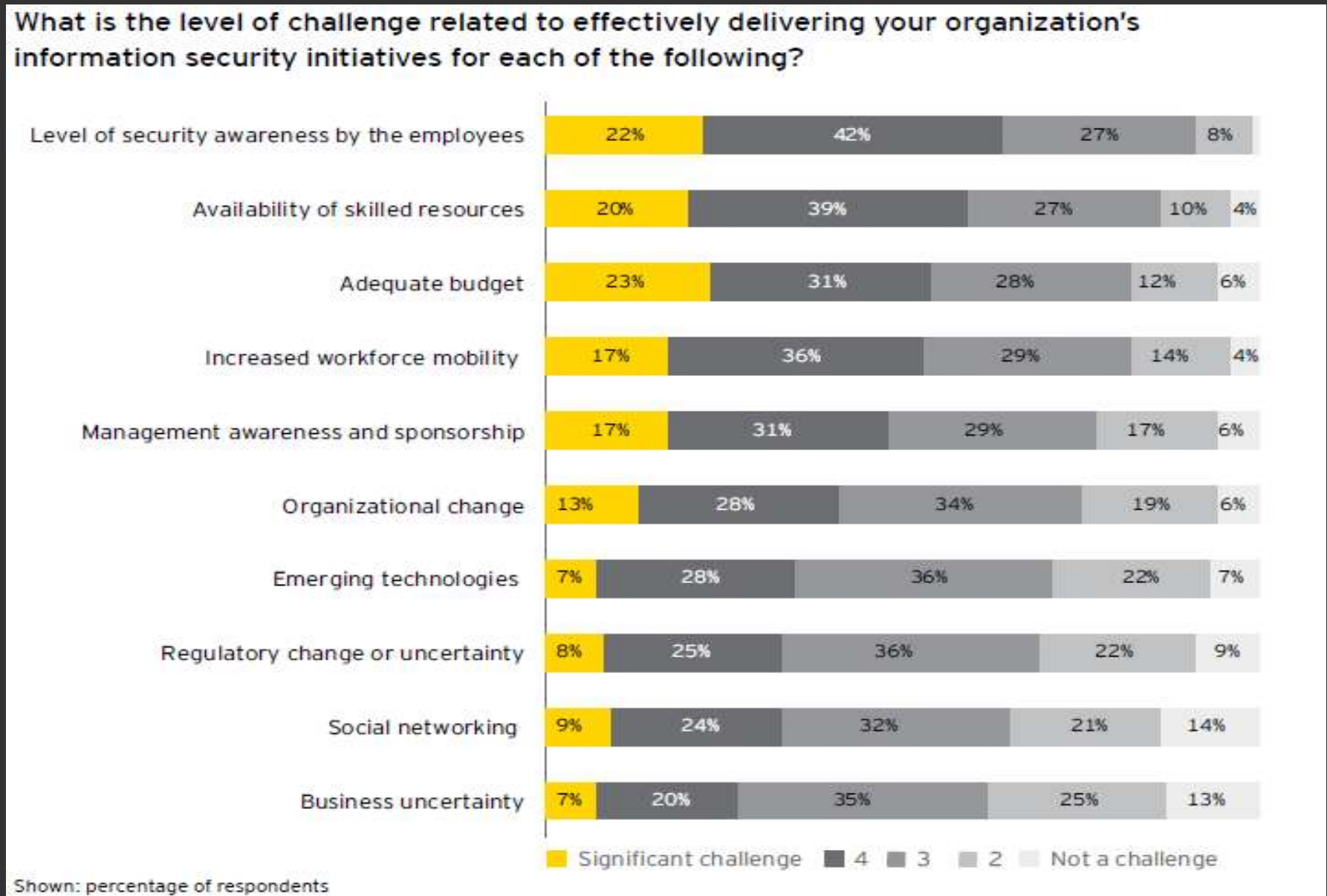
EY 2010 Infosec Survey Selected Findings – Borderless Security

"The trend toward anywhere, anytime access to information will continue changing the business environment, blurring the lines between home and office, co-worker and competitor, and removing traditional enterprise boundaries."

Areas of focus

- Data on the move
  - Mobile workforce
  - Mobile computing risks
  - Plugging the leak
- Processing in the clouds
  - Cloud computing trend
  - Cloud computing risks
  - Securing the cloud
- Web connections
  - Social media
  - Identifying social media risks
  - Securing social behaviour

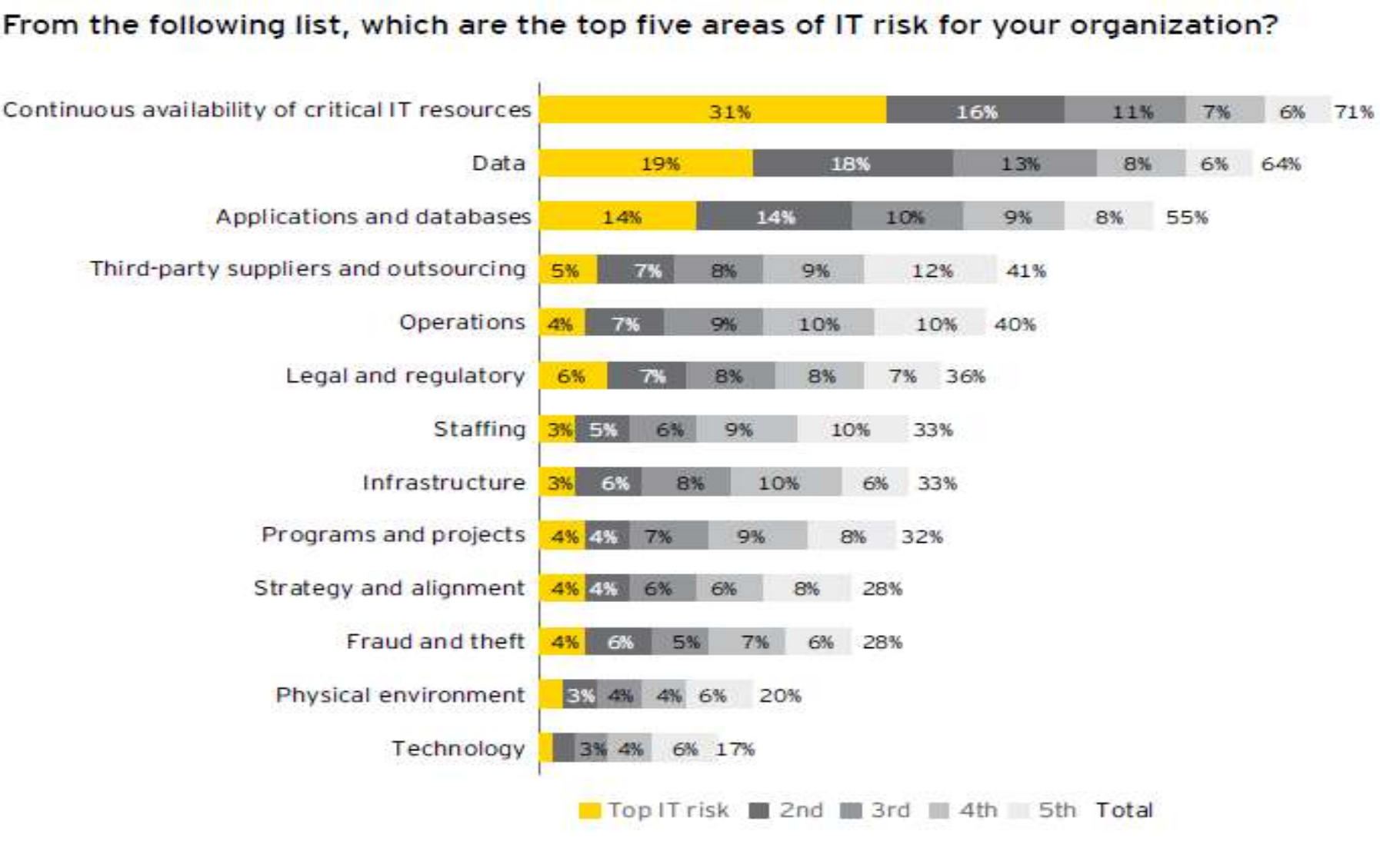
Data on the move



Mobile risk

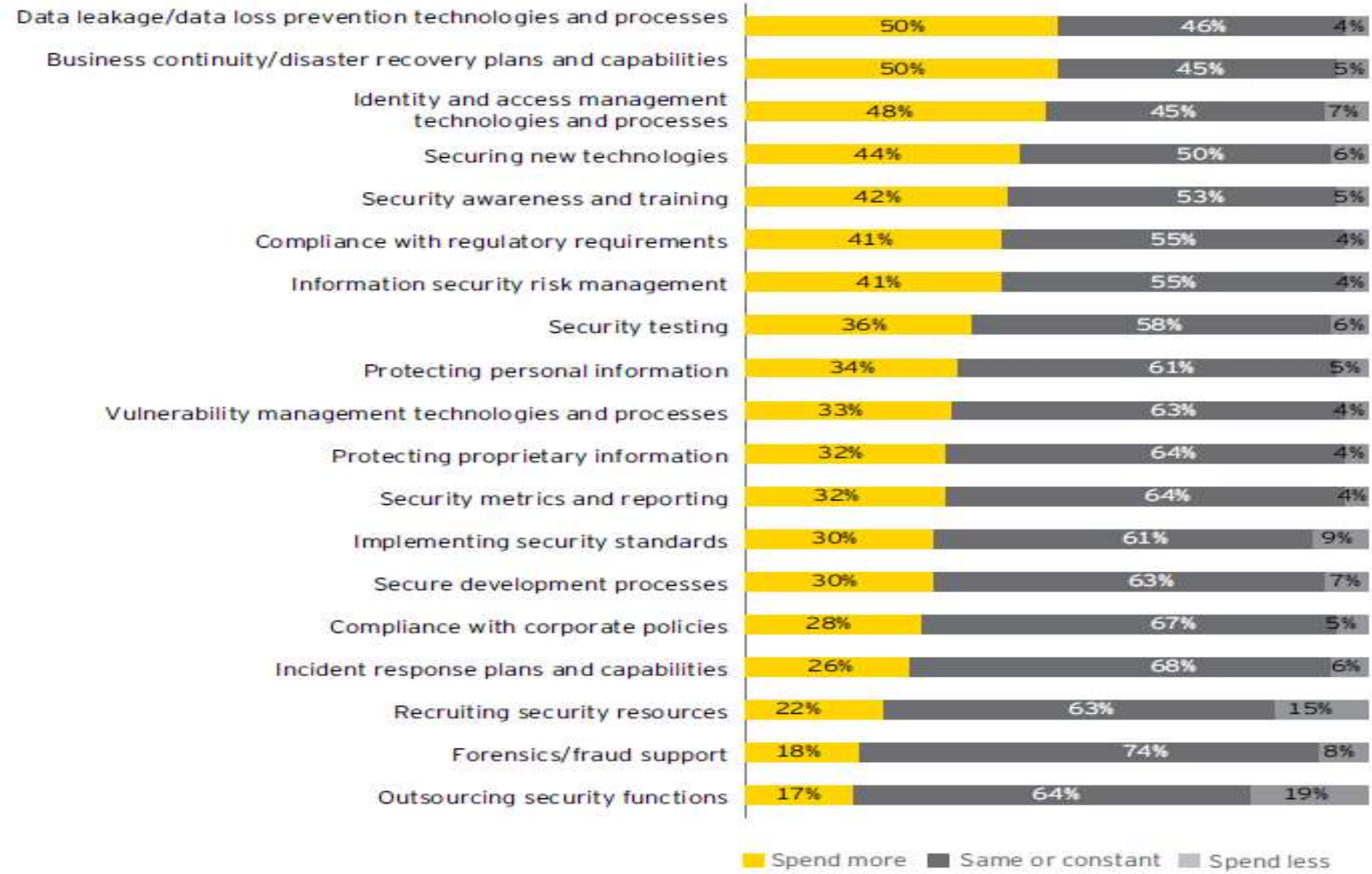
- The increased use of mobile computing devices for business purposes poses serious risk
- Popularity and widespread use of these devices has led to the unwanted, but predictable results:
  - a target for computer viruses and sophisticated mobile malware
  - due to the small size of the portable devices, 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

Data is 2nd highest risk

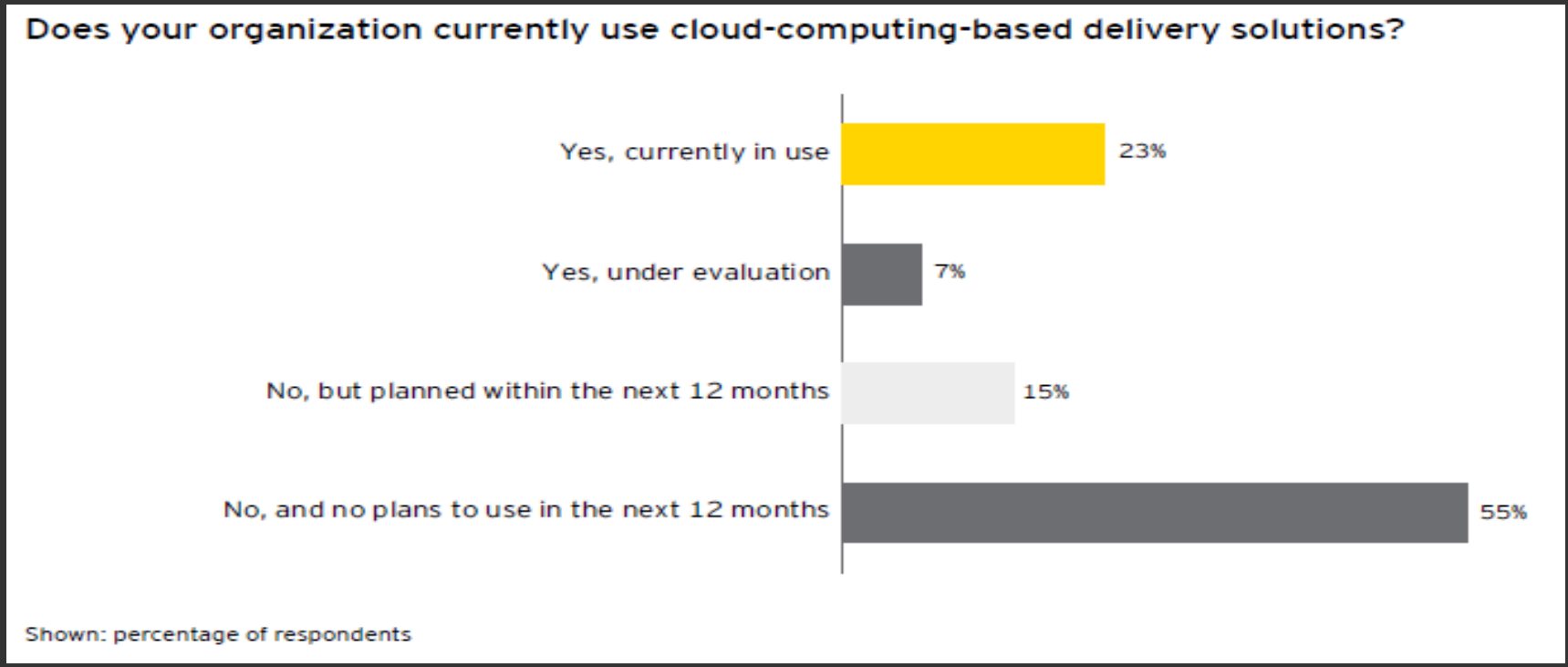


Spend on InfoSec

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the next year for the following activities?



Plans for the cloud

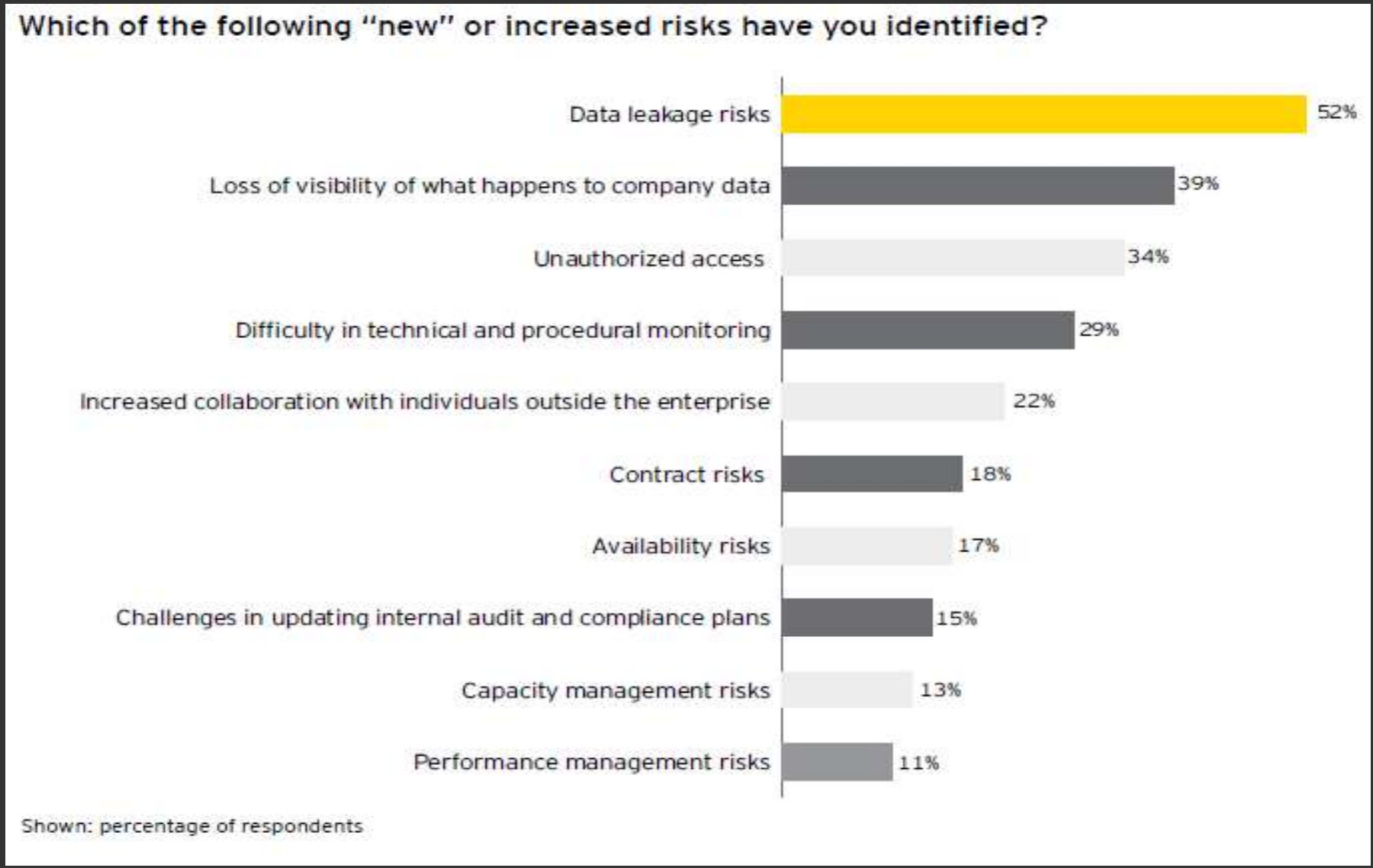


Surprisingly high number

- reliability and security level of many cloud services is still unknown.

Despite an unproven track record, we expect cloud services to increase over the next few years as performance and benefits are demonstrated, offerings and capabilities expand, and cost-cutting pressures continue to force companies to look for alternative IT solutions.

Risks of cloud



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.

CSI FBI 2008 Survey : Overview

- 522 computer security practitioners in the USA
- 13th year of survey
- www.gocsi.com

The most expensive computer security incidents were those involving financial fraud…

…with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with "bot" computers within the organization's network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.

Virus incidents occurred most frequently…

…occurring at almost half (49 percent) of the respondents' organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

Almost one in ten organizations reported they'd had a Domain Name System incident…

…up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.

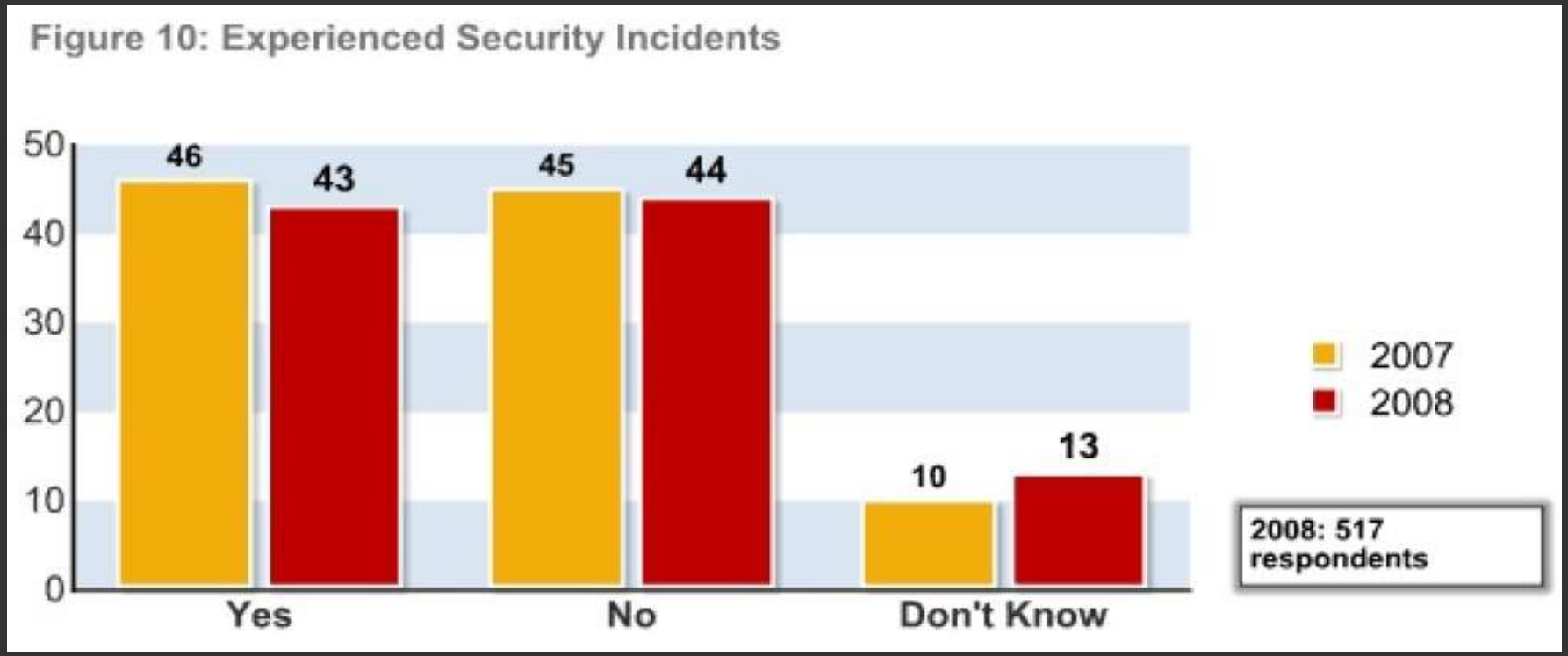
Twenty-seven percent of those responding to a question regarding "targeted attacks"…

…said they had detected at least one such attack, where "targeted attack" was defined as a malware attack aimed exclusively at the respondent's organization or at organizations within a small subset of the general business population.

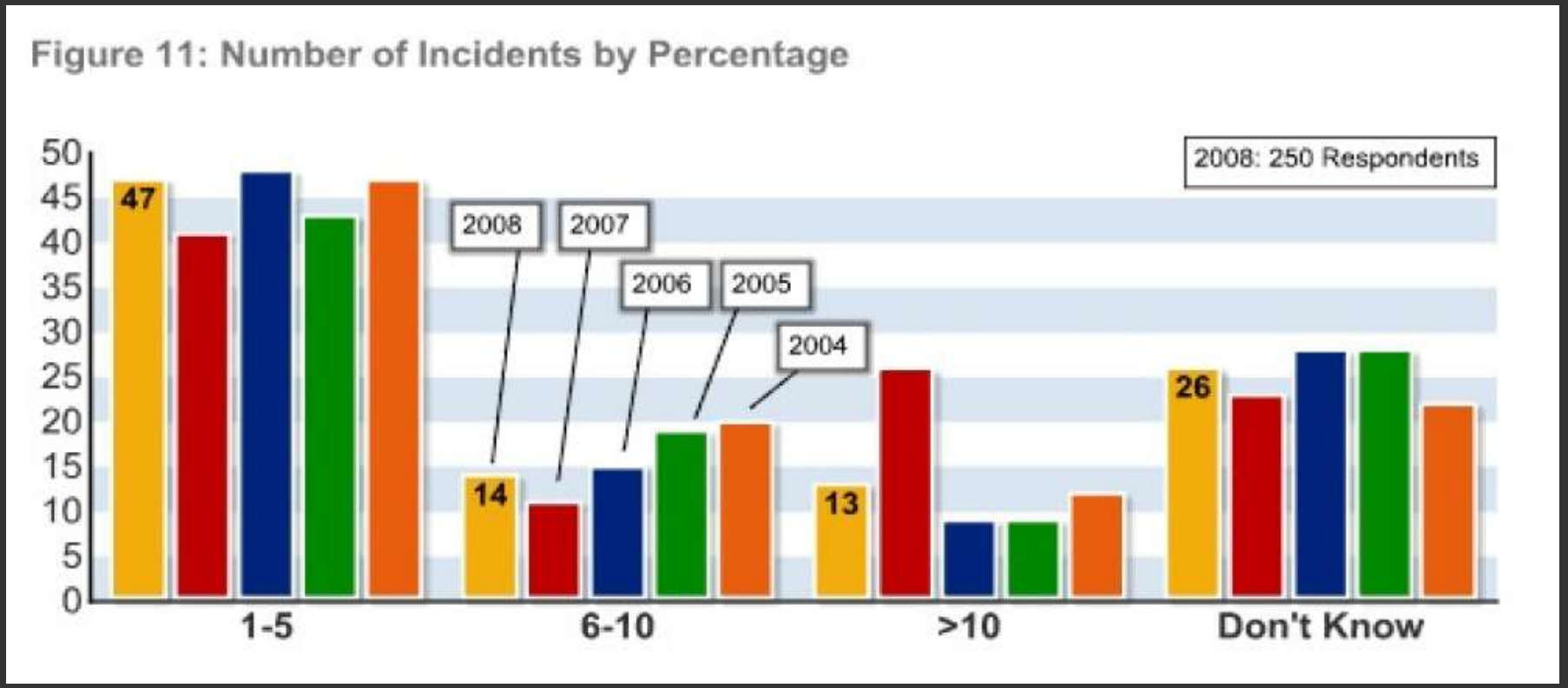
The vast majority of respondents said their organizations either had (68 percent)…

…or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.

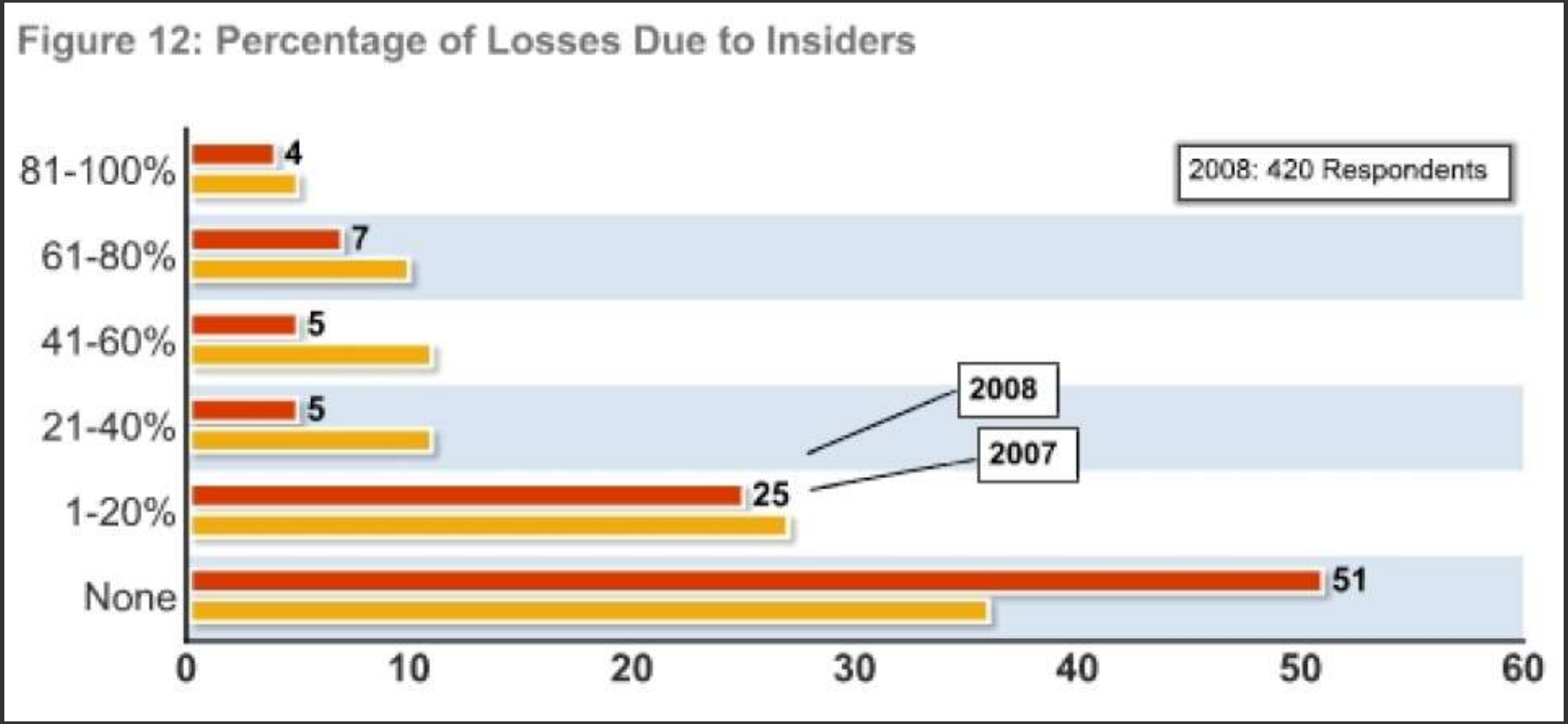
CSI FBI 2008 Survey : Experienced Security Incidents



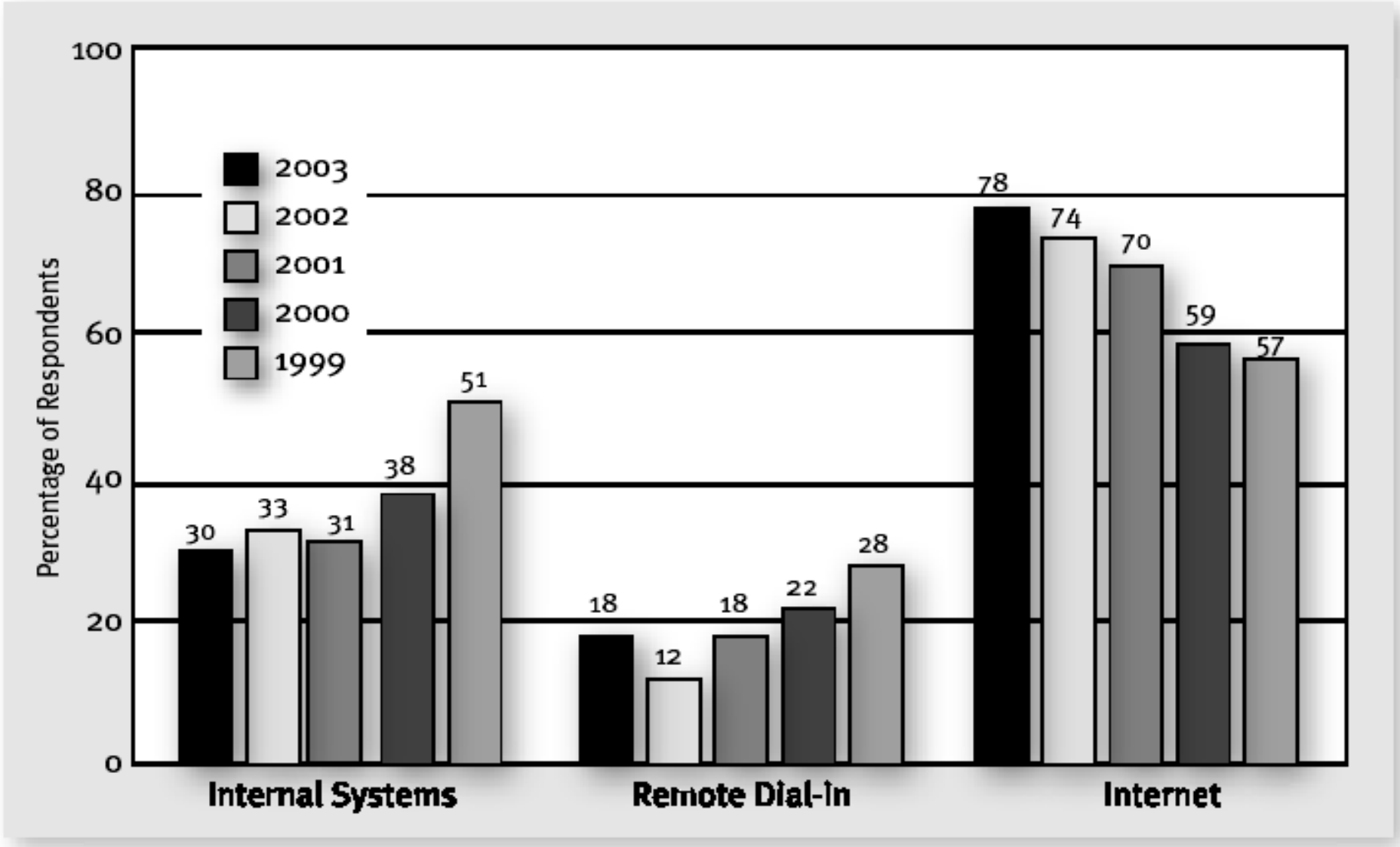
CSI FBI 2008 Survey : Number of incidents



CSI FBI 2008 Survey : Loss from insiders

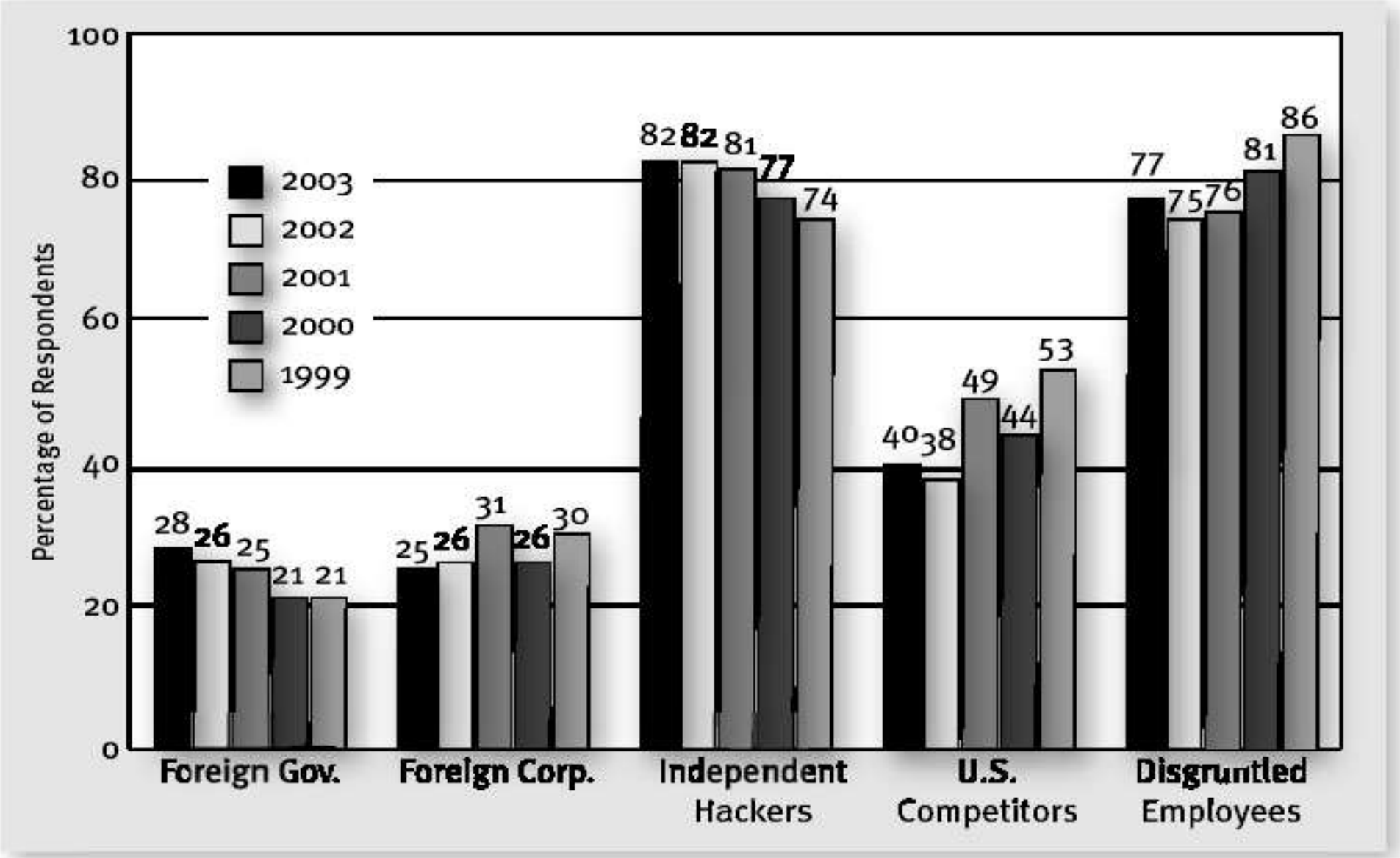


Internet Connection is Increasingly Cited as a Frequent Point of Attack



CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

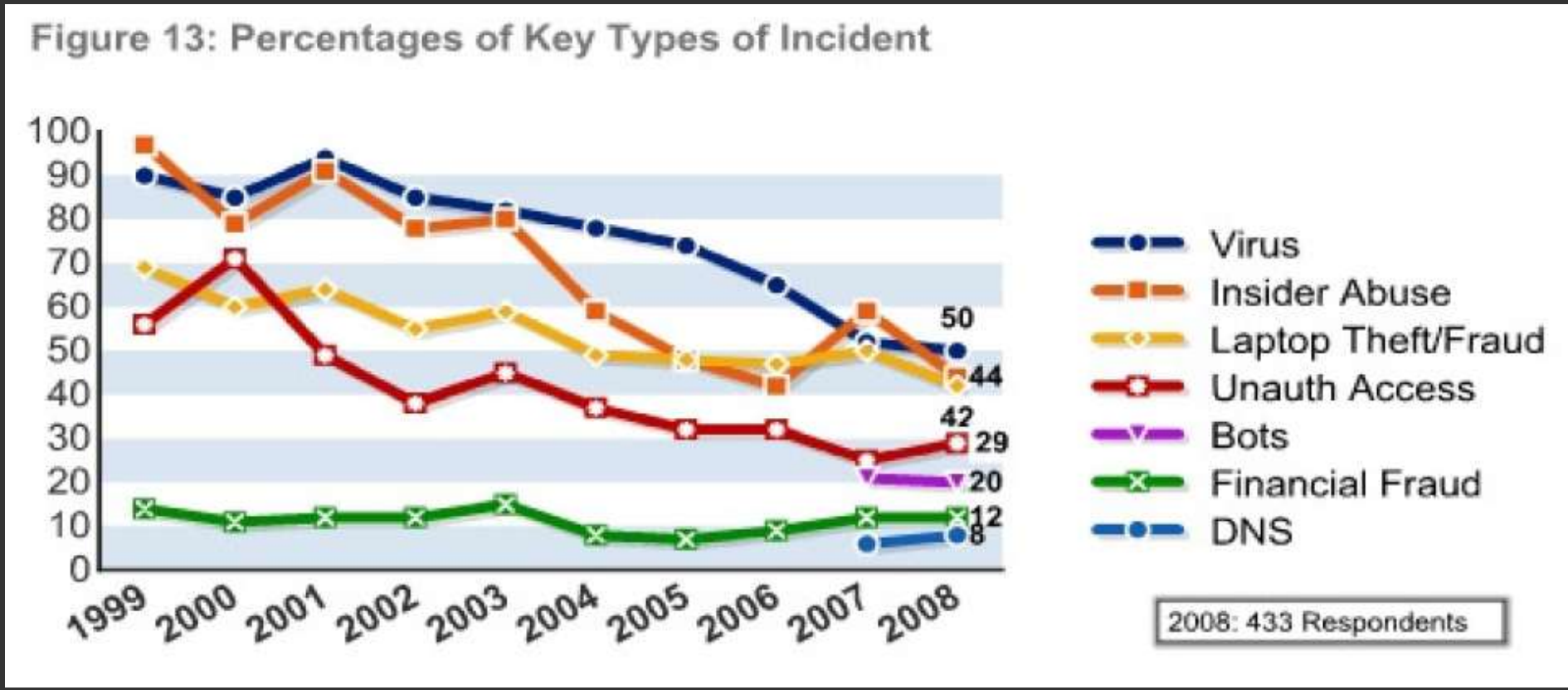
Likely Sources of Attack



CSI/FBI 2003 Computer Crime and Security Survey

Source: Computer Security Institute

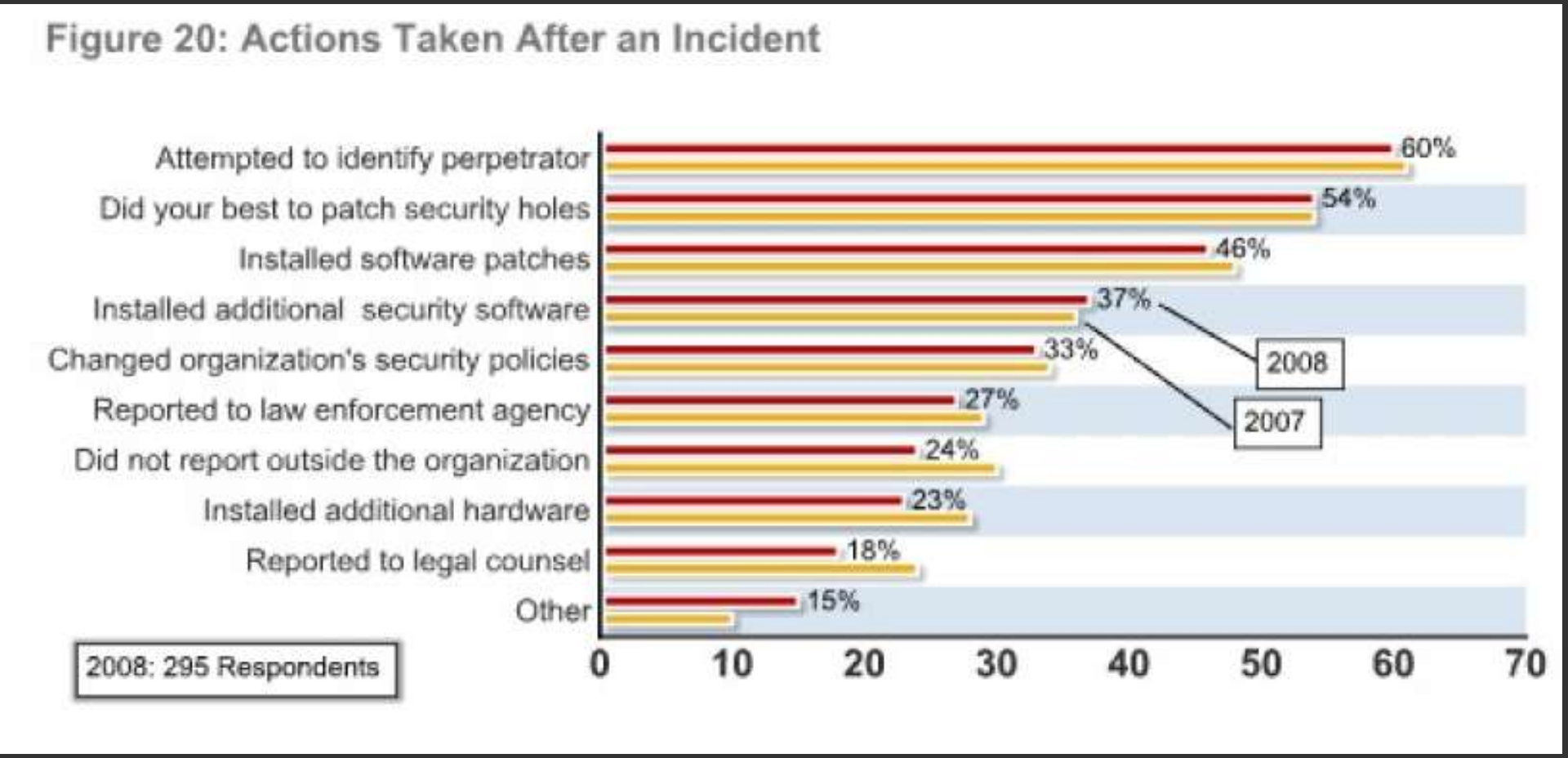
CSI FBI 2008 Survey : Types of incidents



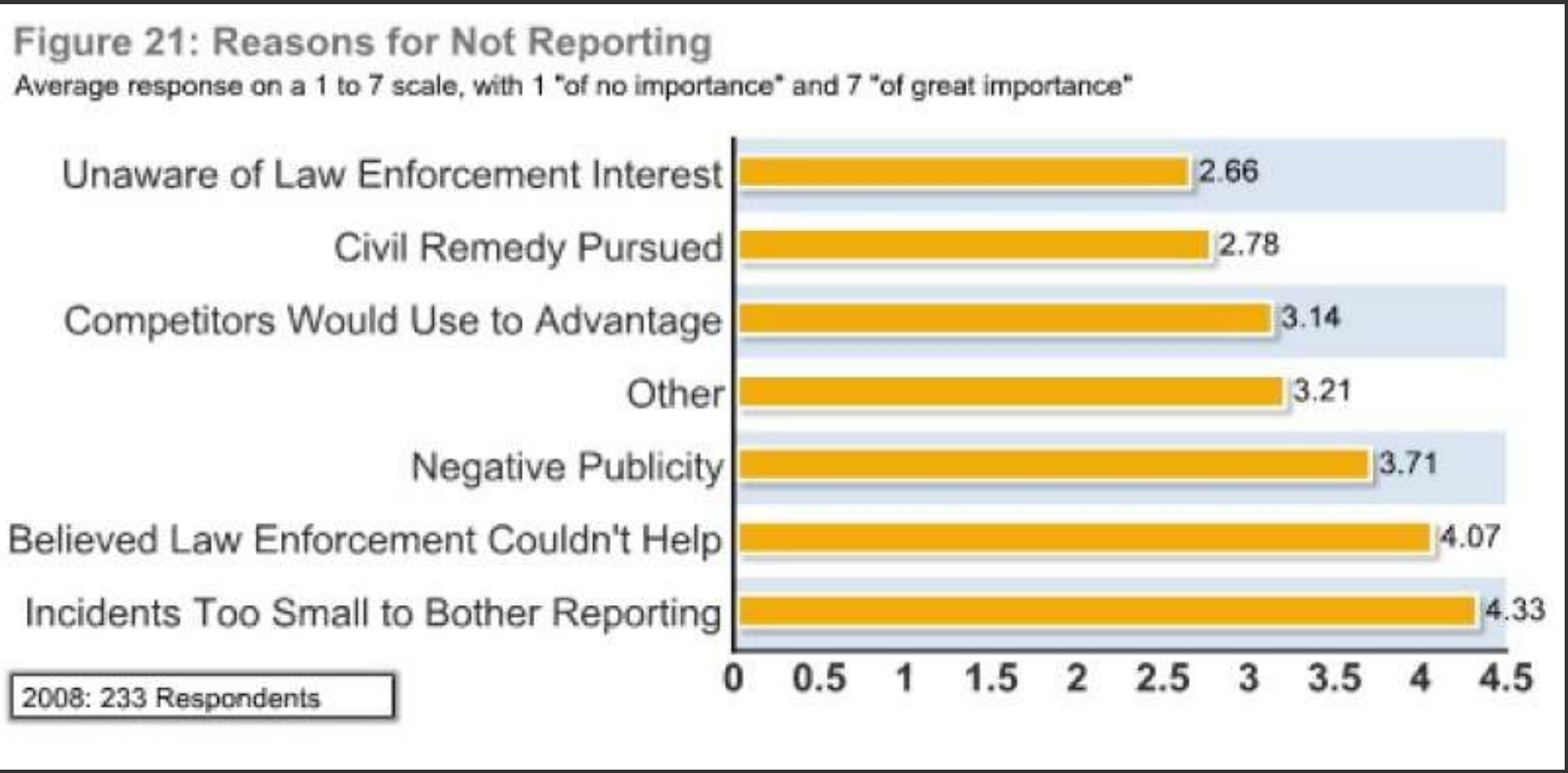
CSI FBI 2008 Survey : Types of incidents

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

CSI FBI 2008 Survey : Actions taken after incident



CSI FBI 2008 Survey : Why not report



Cost of computer security breaches

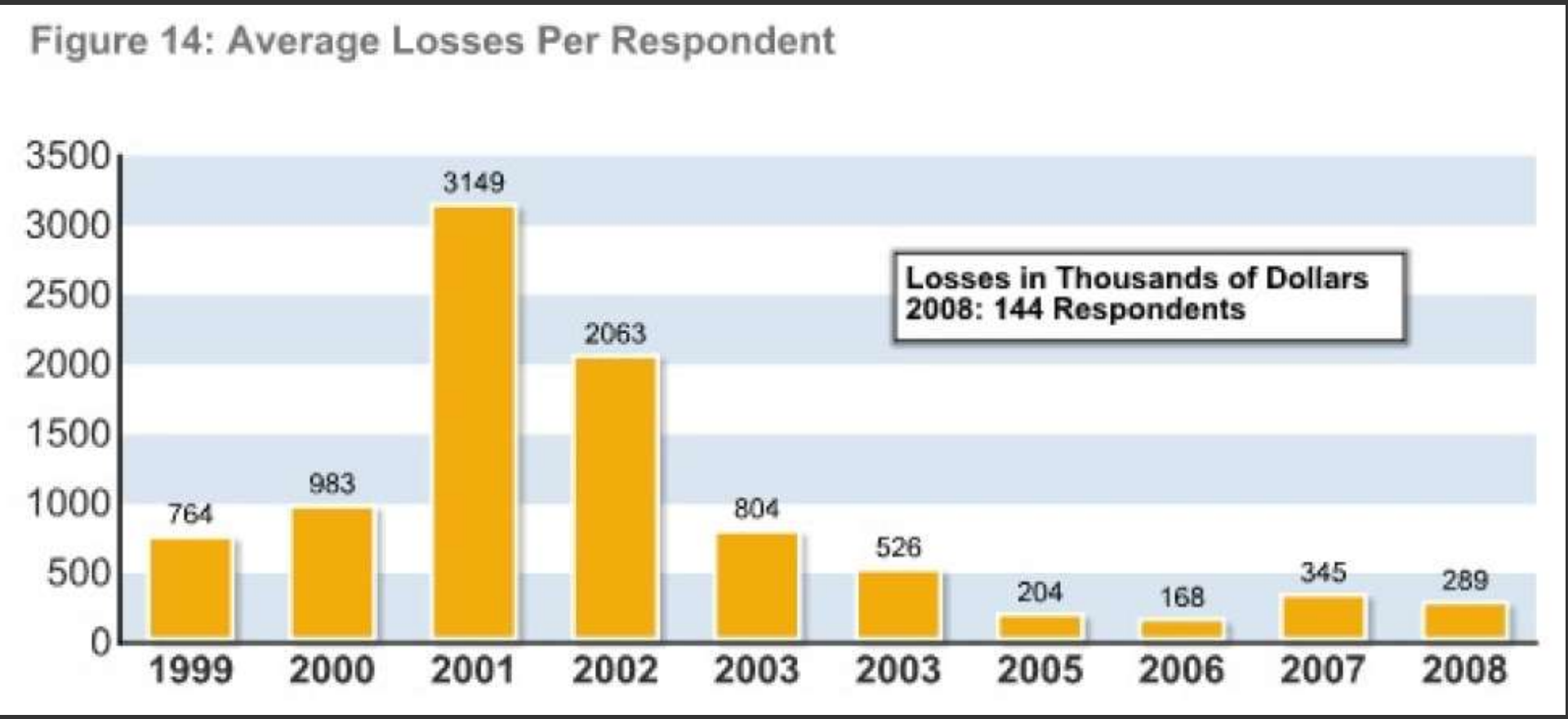
- 80% of organisations acknowledged financial loss as a result of a computer breach.
- 44% were willing and/or able to quantify their financial loss
- Most serious financial loss as a result of theft of proprietary information and financial fraud
  - Theft of proprietary information and financial fraud 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 …

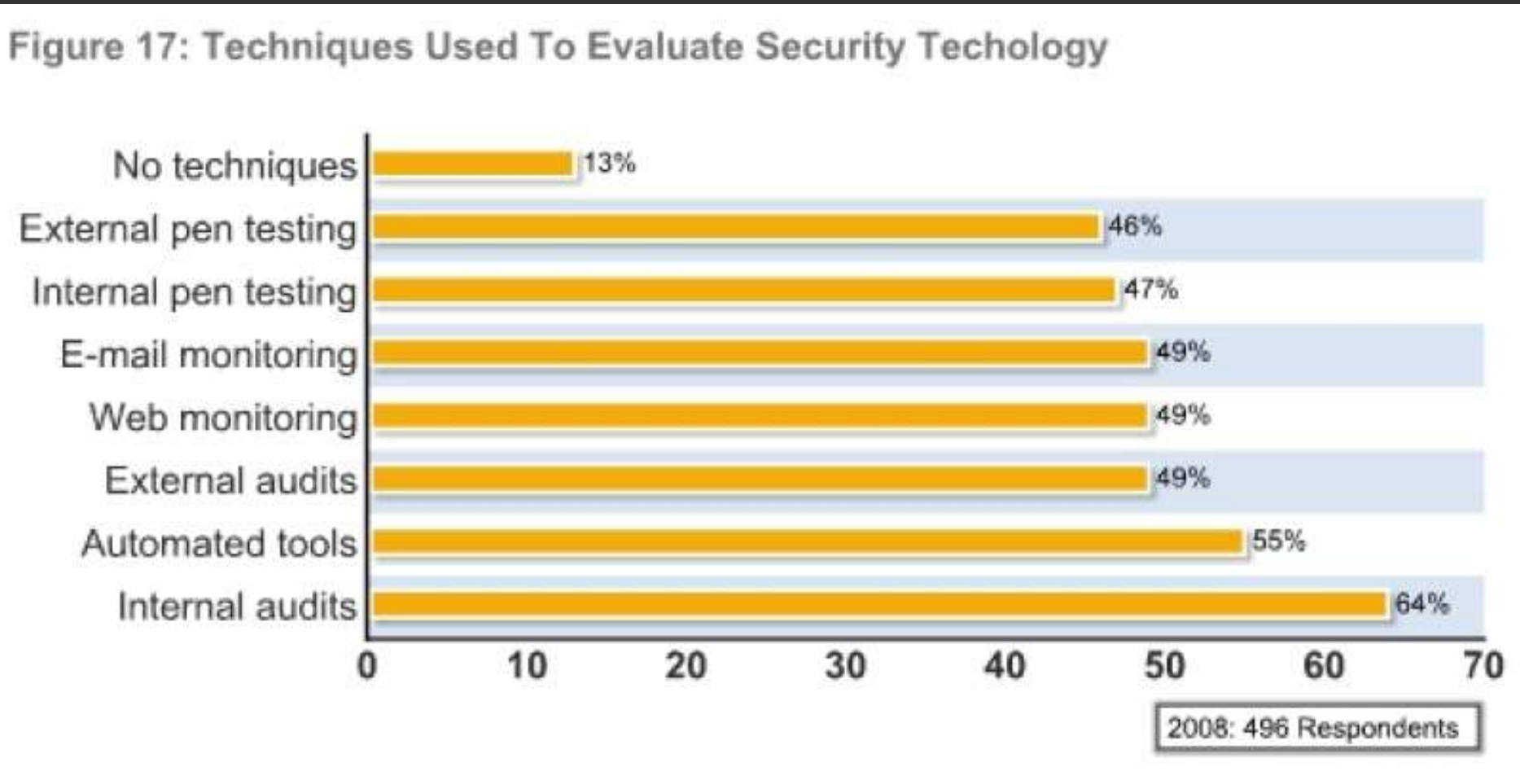
- Trend moved downwards (per CSI/FBI)
  - $289k average incident loss, still down from early 2000's
  - Highest Average loss $3,149k in 2001

- 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)

CSI FBI 2008 Survey : Loss per incident



CSI FBI 2008 Survey : Evaluating Security



"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?

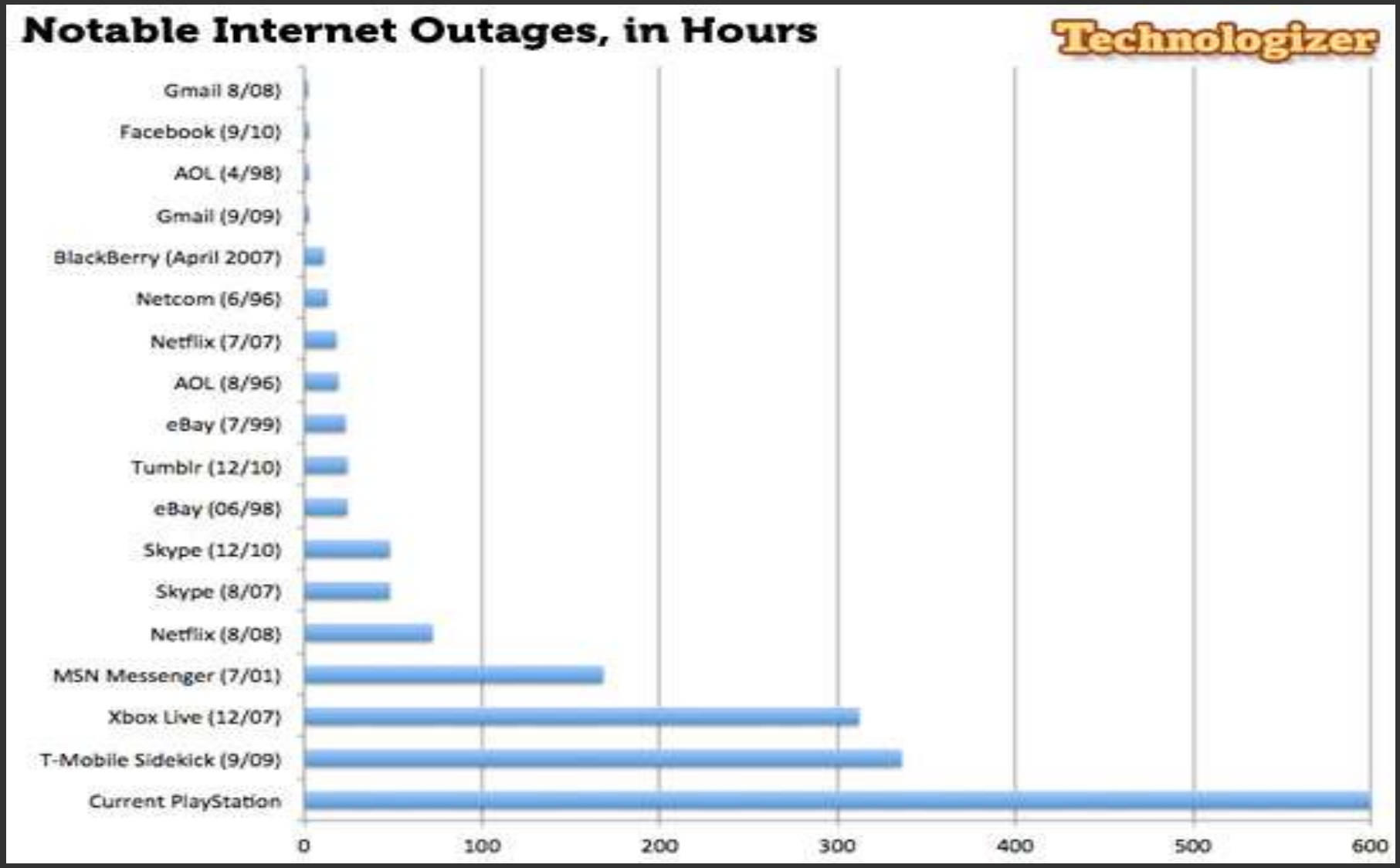
Sony: The Company That Kicked the Hornet's Nest

Biggest failure of the decade?

- An April 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

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 Mar. 3.
  - 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 Apr. 15, 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?

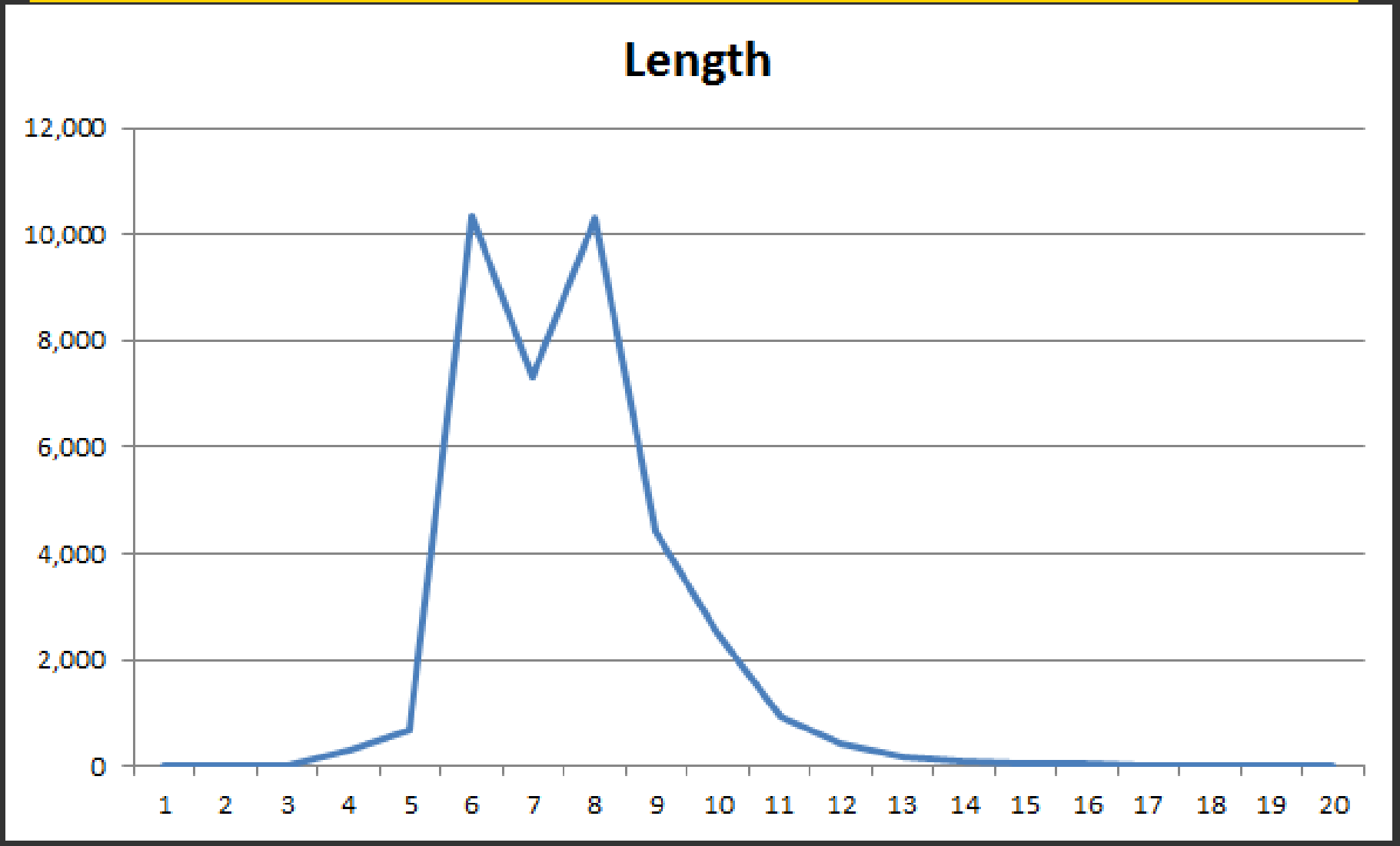
But wait, there is more ....

Analysis of hacked passwords

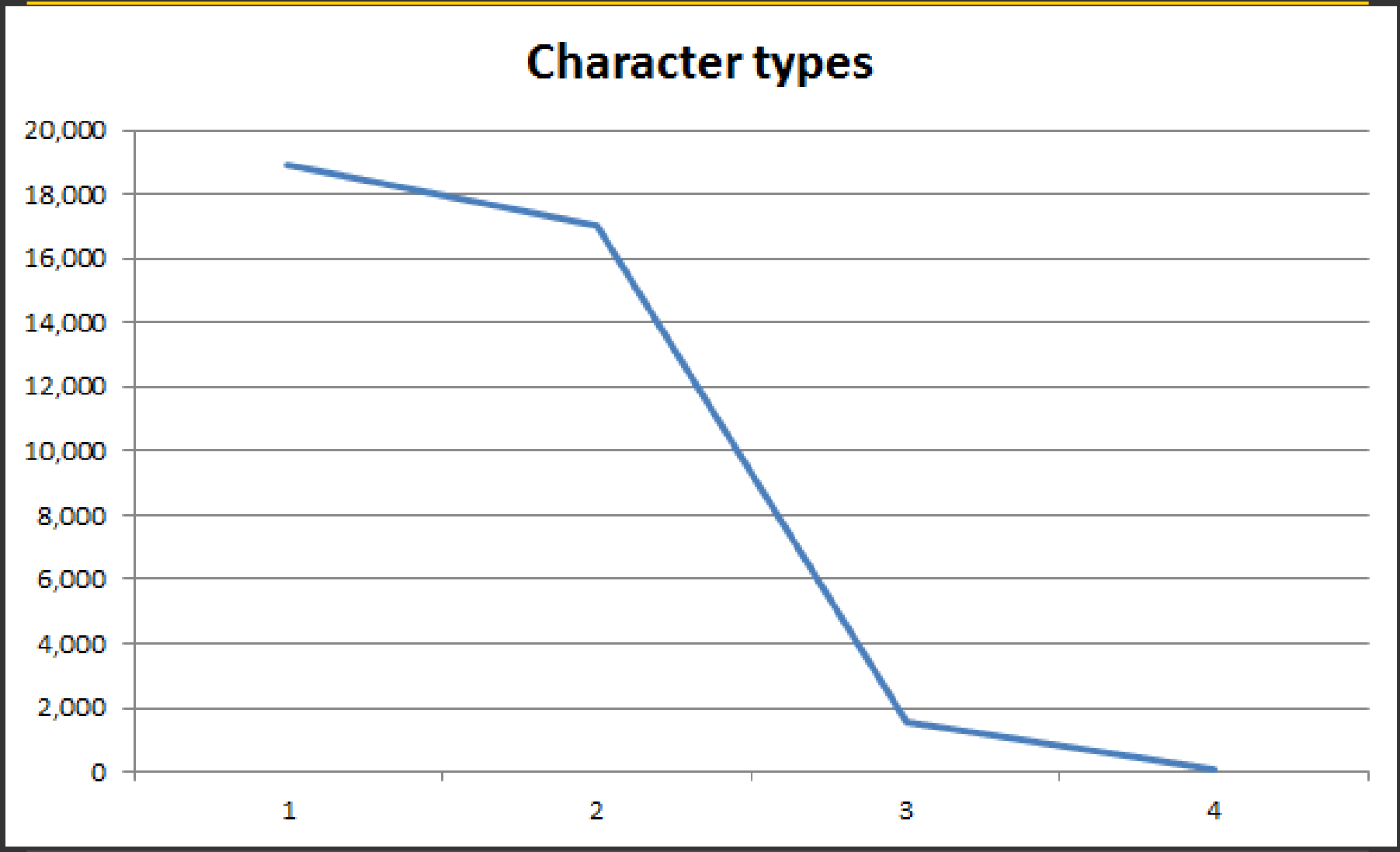
- Troy Hunt analysed password released by Anonymous

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

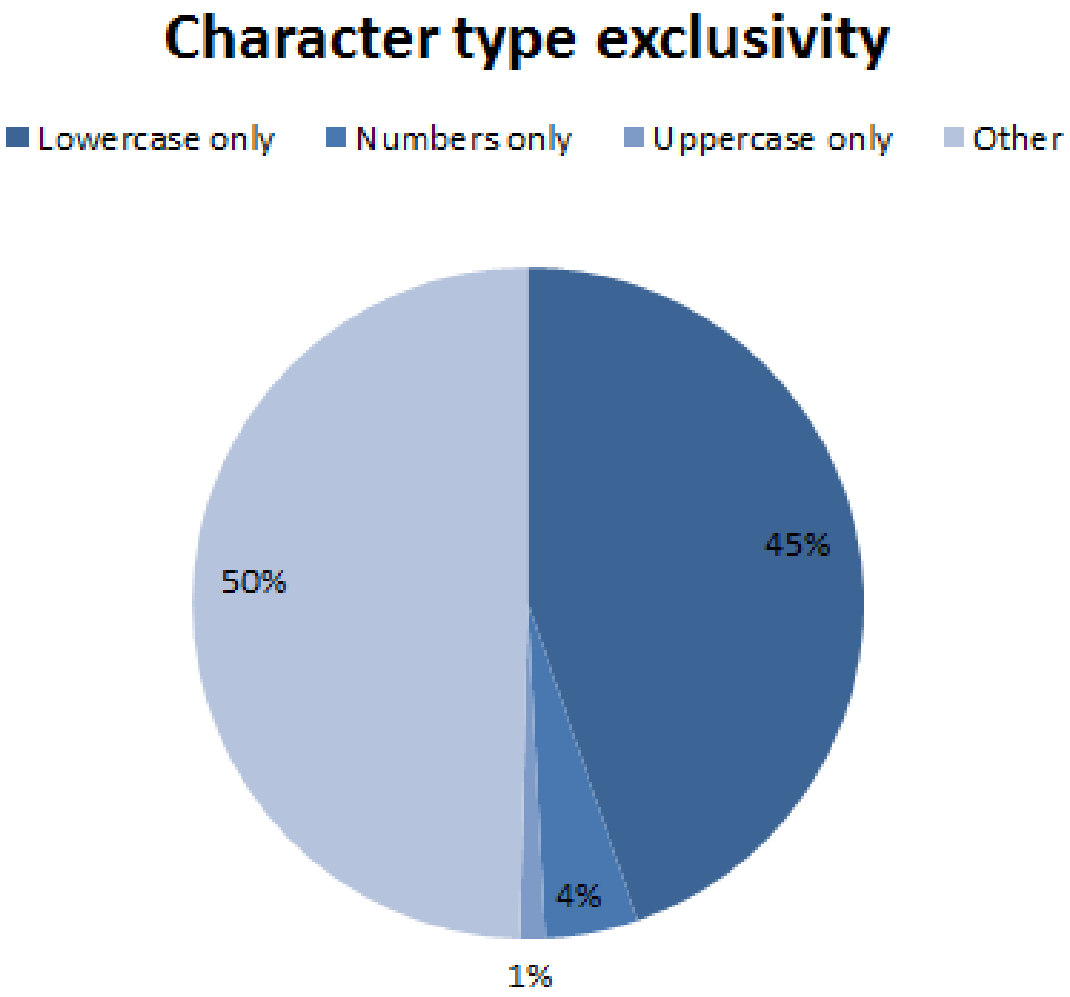
Password Length



Character Types

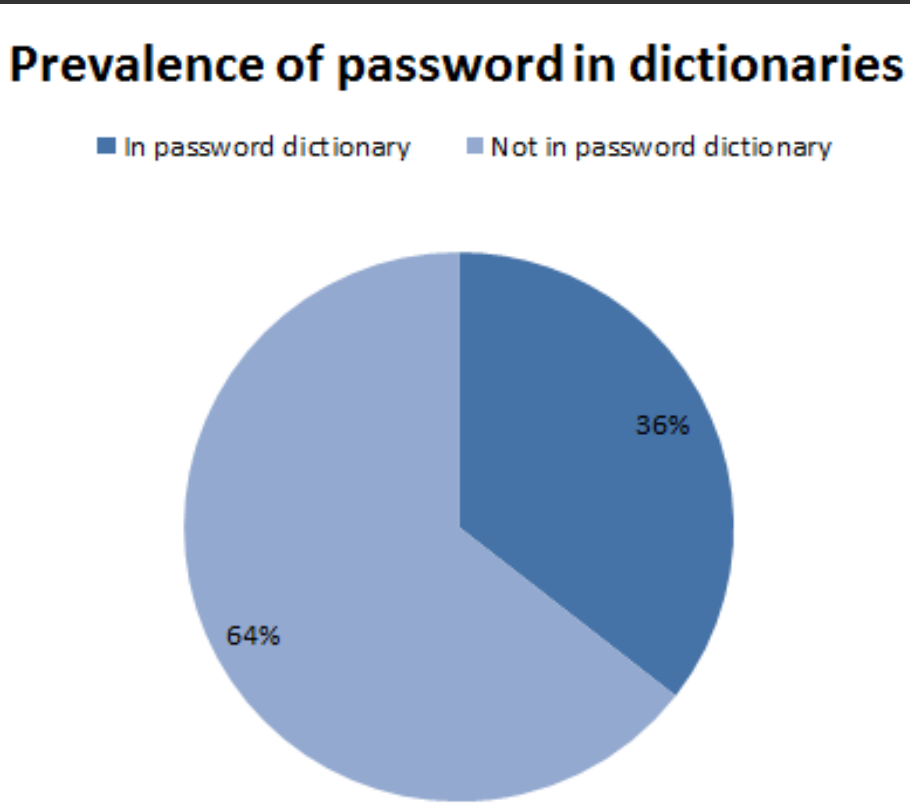


Character Type Exclusivity

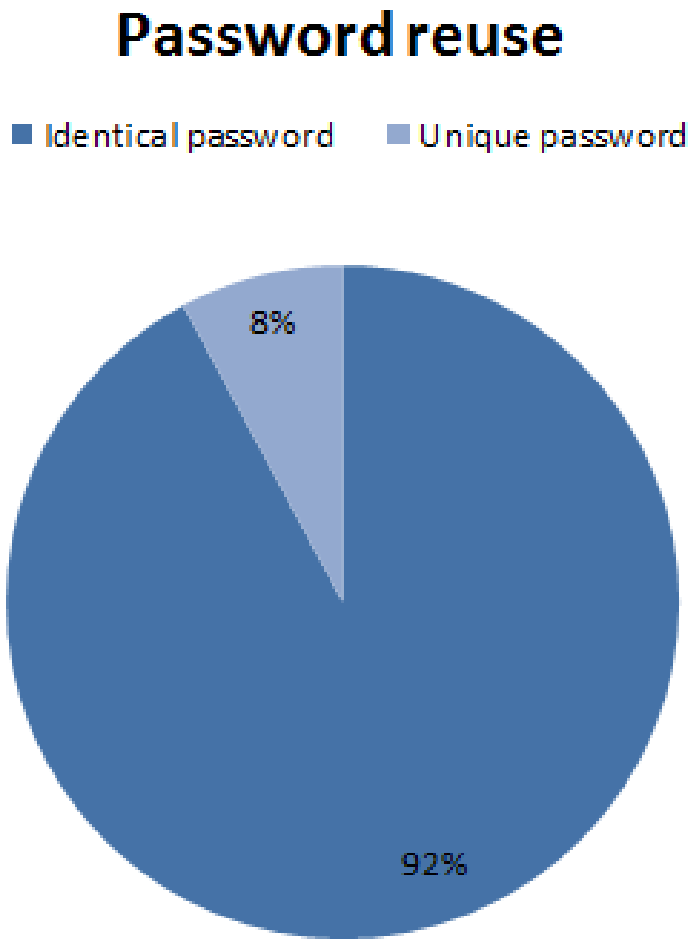


Randomness

- 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.*
- 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: Lulz8ec published the names, birthdates, phone numbers, and email addresses of an estimated 280,000 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 5134 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.

Embarrassing 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 damage done to active FBI.

B

June 6th: "Sownage Part 2"

The Target: Sony Computer Entertainment Developer Network

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

Well-executed, but damage is difficult to access.

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

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
  - 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!!!

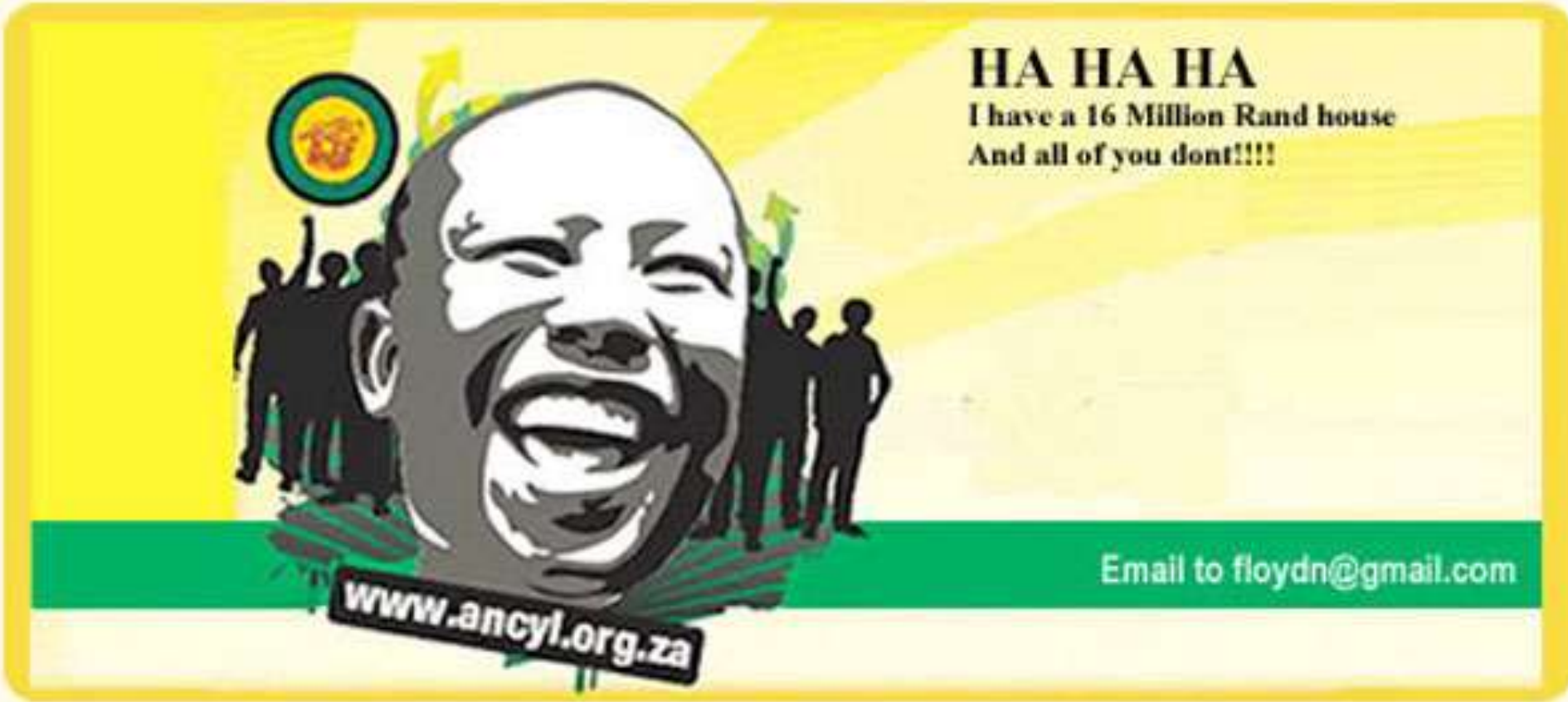
E1231N2 ENQUIRY ON A CANDIDATE
E1231PE SENIOR CERTIFICATE (FULLTIME) - 200

Centre..: A 7150119 Exam no.: 172501190042 Valid
Date of birth: 19810303 Mother tongue.:
MALEMA JULIAS SELLO

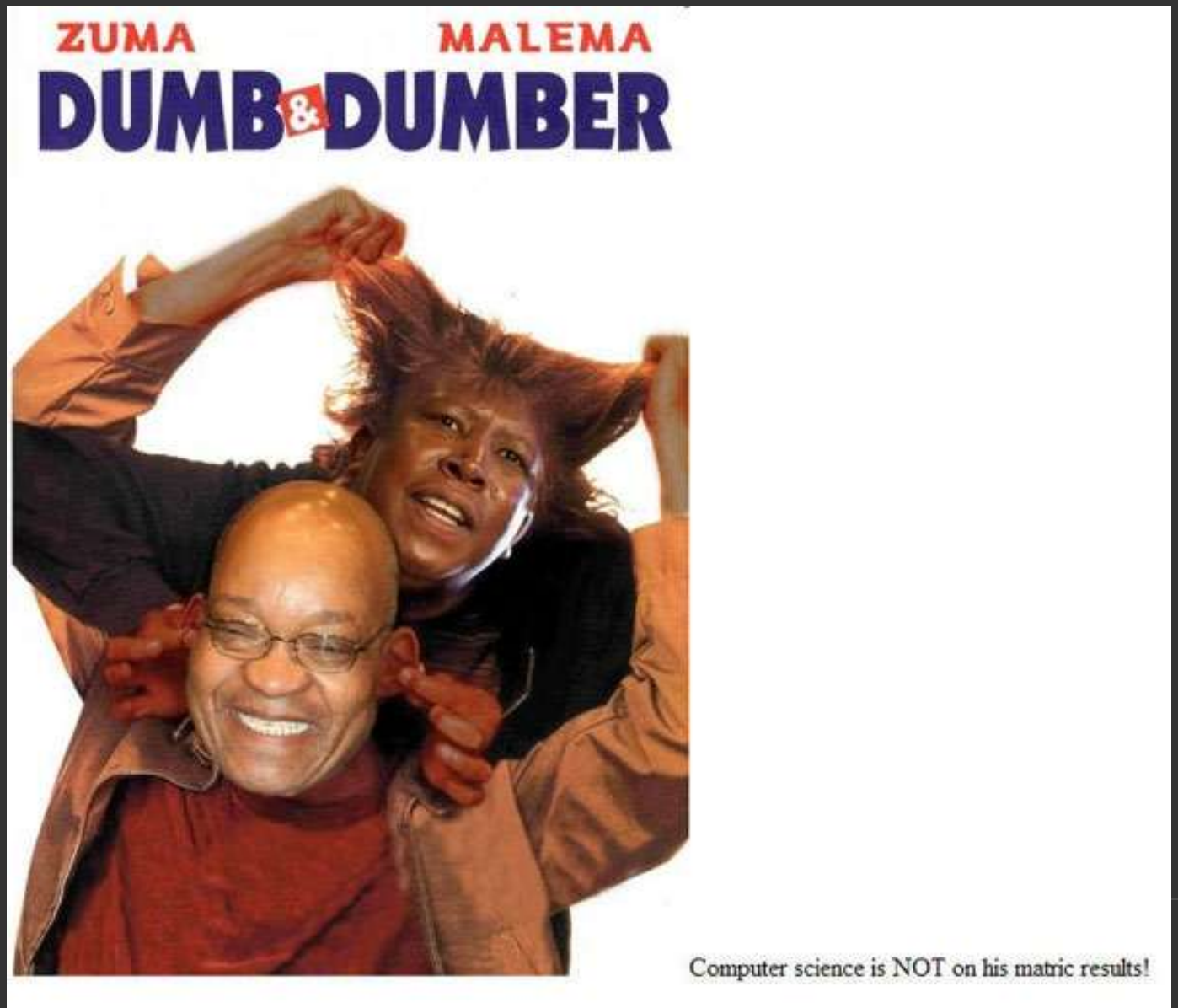
Subj.	Subject Description	Grp	Mark	Symbol	
1	SEPEDI FIRST LANGUAGE H	A1	134	B	X
12	AFRIKAANS SECOND LANGUA	A2	128	B	
15	ENGLISH SECOND LANGUAGE	A2	180	C	
39	GEOGRAPHY HG	E6	129	F	O
46	HISTORY SG	E6	170	D	
64	WOODWORKING SG	F7	72	GG	
18	MATHEMATICS SG	B3	12	H	

No of Subjects: 7

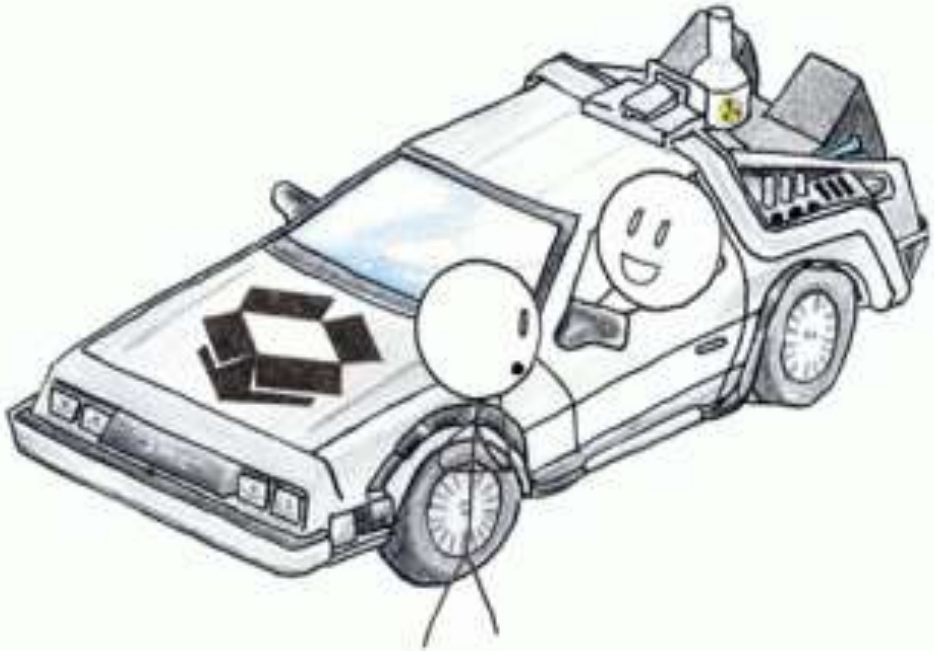
Third – 24 July 2011



Fourth – 26 July 2011



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).

Download Dropbox

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

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

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

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.

- **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.

- **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

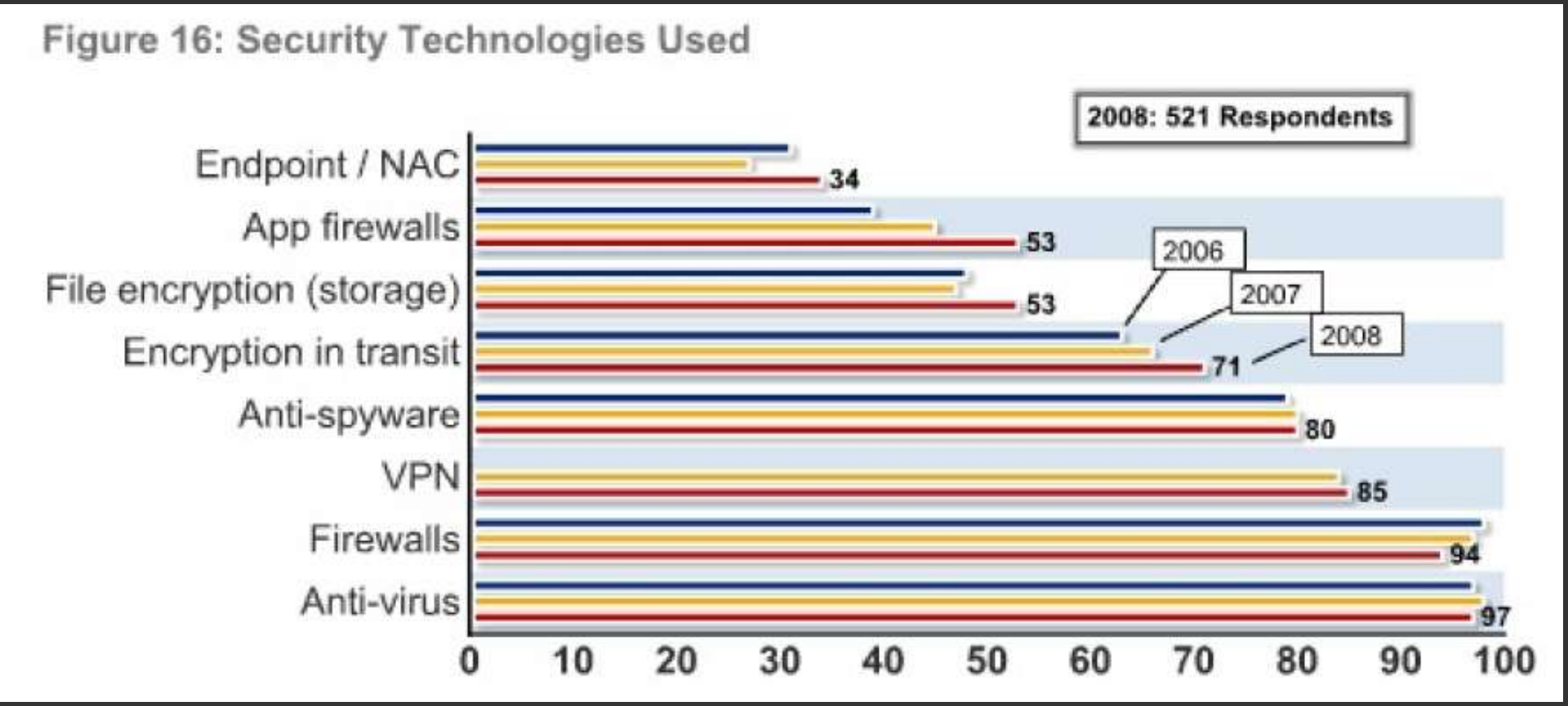
- **Other social engineering methods:**
  - Handing out memory sticks
  - Facebook / Linkedin / Twitter

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
    - 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

CSI FBI 2008 Survey : Technology used



CSI FBI 2008 Survey : Technology used

Table 2: Technologies Used	2008
Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
Firewalls	94 %
Forensics tools	41 %
Intrusion detection systems	69 %
Intrusion prevention systems	54 %
Log management software	51 %
Public Key Infrastructure systems	36 %
Server-based access control lists	50 %
Smart cards and other one-time tokens	36 %
Specialized wireless security systems	27 %
Static account / login passwords	46 %
Virtualization-specific tools	29 %
Virtual Private Network (VPN)	85 %
Vulnerability / patch management tools	65 %
Web / URL filtering	61 %
Other	3 %

Biggest Issues for South African Companies

- Strategic
  - Privacy
  - 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
- Procedural
  - Ongoing compliance
  - Poor administrative practices
  - User Education

Next big things

- Smart code
  - Trojans / worms bypass current security measures
  - Embedding the code in the web browser
    - Commits actions on behalf of user (withdraw funds)
    - Changes what is displayed (fraudulent transactions eliminated)
  - Exploits end user applications : Windows Media Player, Winamp, Mirc or any others
  - Machines “protected” by corporate firewalls are accessible to hackers on the outside
- Cloud computing
  - Ownership and data security
  - Business continuity
  - Ability to switch service providers

Next big things

- Hacking “other” Network devices
  - Printers
  - Routers, switches, gateways
  - PABX Systems
  - Voice over IP
  - Mobile devices (Blackberry etc)
- Higher application layers
  - Databases
    - Automated tools already available to attack databases and web based applications (Eg. DataThief)
  - Application specific attacks
    eg. Recent SCADA attacks

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.williams@transnet.net
- Mobile : 082 772 9881
- Website : http://j-j.co.za
-  @jjza http://twitter.com/jjza
-  Justin Williams, Durban, SA

Ernst & Young's 2009 Global Information Security Survey

The EY security survey is one of the longest-running and most recognized annual surveys of its kind. For 12 years, our survey has helped our clients focus on the right risks and priorities, identify their strengths and weaknesses, and improve their information security. This year's survey received the highest levels of participation since inception.

In this survey we take a closer look at how organisations are specifically addressing their information security needs. We also identify and summarise potential opportunities for improvement and important trends that will continue to drive information security in the coming years.

How do you protect your organization's brand and reputation in an environment of change? How do you identify and manage new risks? How do you overcome increasing challenges to deliver an effective information security program? How do you comply with new regulations and industry requirements? How do you leverage technology to not only meet business objectives but also improve security?

2009 Global Security Survey

Key survey findings

Managing risks

- Improving information security risk management is a top security priority for the next year.
- External and internal attacks are increasing.
- Reprisals from recently separated employees have become a major concern.

Addressing challenges

- Availability of skilled information security resources is the greatest challenge to effectively delivering information security initiatives.
- Despite most organizations maintaining current spending on information security, adequate budget is still a significant challenge to delivering security initiatives.
- Security training and awareness programs are falling short of expectations.

Complying with regulations

- Regulatory compliance continues to be an important driver for information security.
- Cost of compliance remains high, with few companies planning to spend less in the next 12 months.
- Too few organizations have taken the necessary steps to protect personal information.

Leveraging technology

- Implementing DLP technologies is the top security priority for many organizations.
- The lack of endpoint encryption remains a key risk with few companies encrypting laptops or desktop computers.
- Virtualization and cloud computing are gaining greater adoption, but few companies are considering the information security implications.