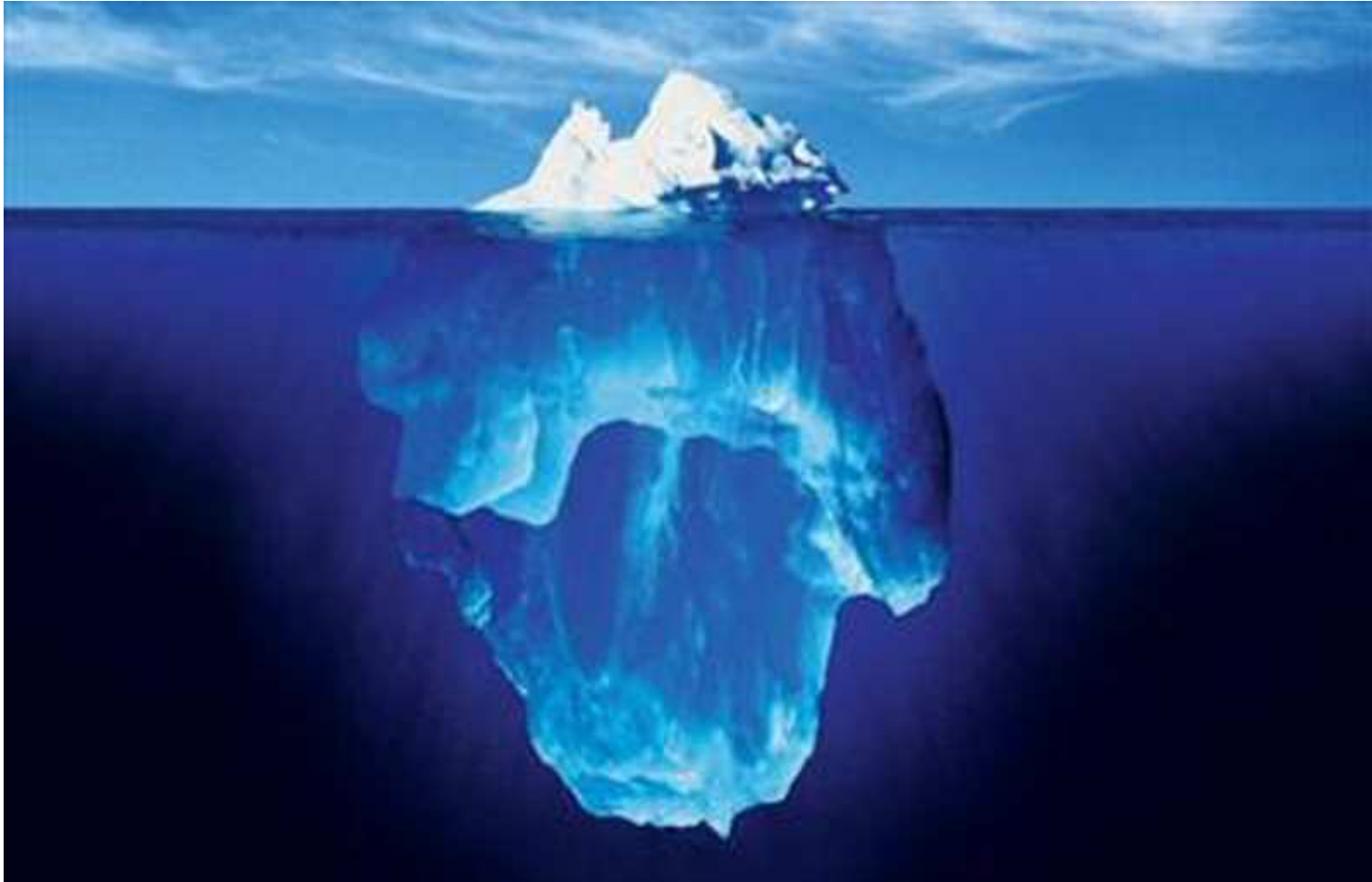




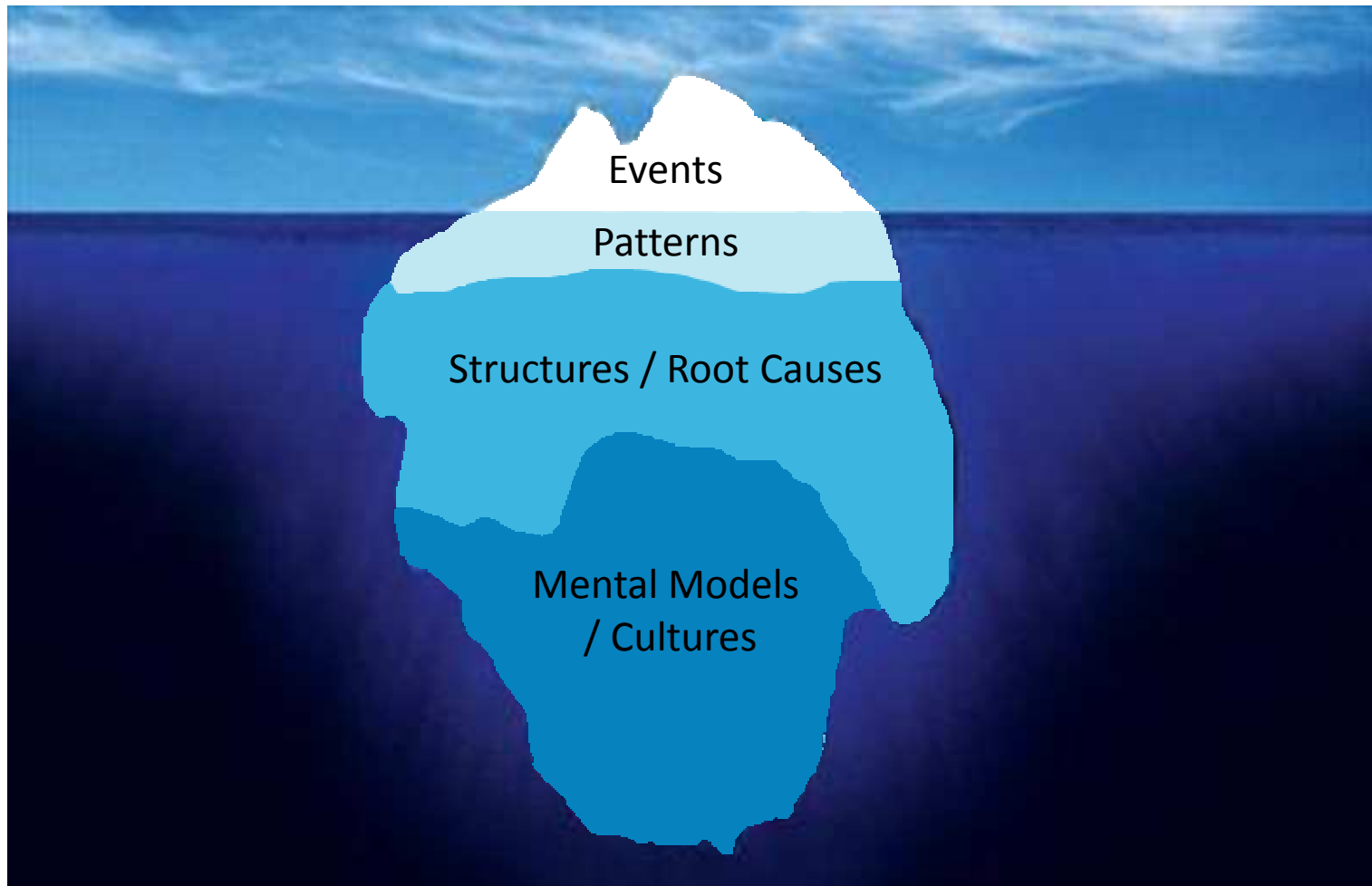
P22 – Top Risks in an IT Environment

Back to Business

The Iceberg Model



The Iceberg Model



IT Risks – Pick Your Poison?



Baseline
10 SECURITY RISKS IN 2011



JUNIPER
NETWORKS

MOBILE DEVICE SECURITY—
EMERGING THREATS,
ESSENTIAL STRATEGIES



SOPHOS
Security threat report 2011

eSecurity Planet
Top 10 Android Security Risks



Attack Vector Evolution

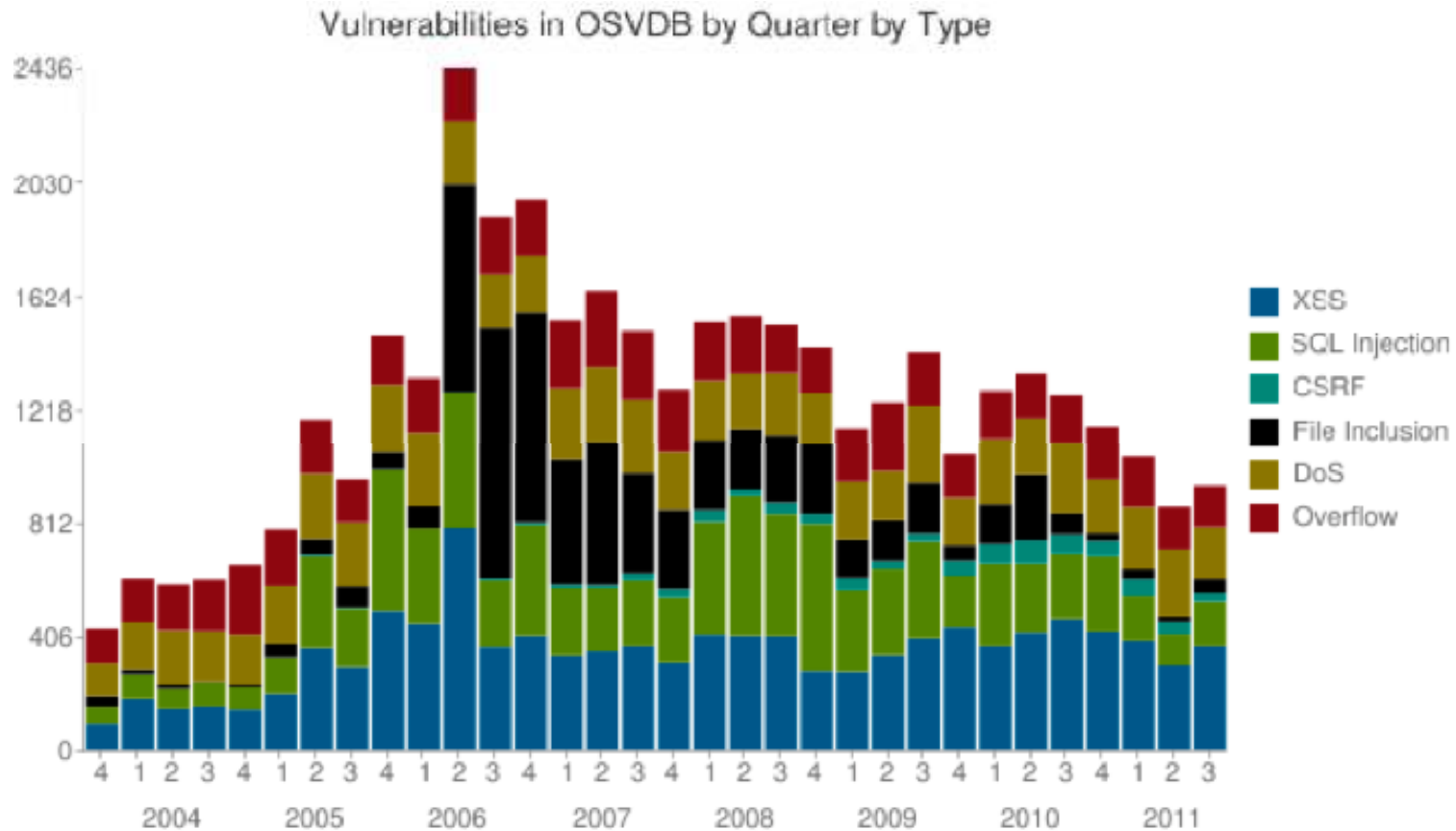


Source: Trustwave

What MY CISO Friends Worry About

- Data loss/breach (IP and/or PII) breach
- Insider threat – malicious or unintentional
- Social engineering (*and* social networking)
- APTs (Advanced Persistent Threats) and other 0-day malware
- Mobile devices
- Buggy code discovered by 3rd party (reputation damage)
- “The Cloud”

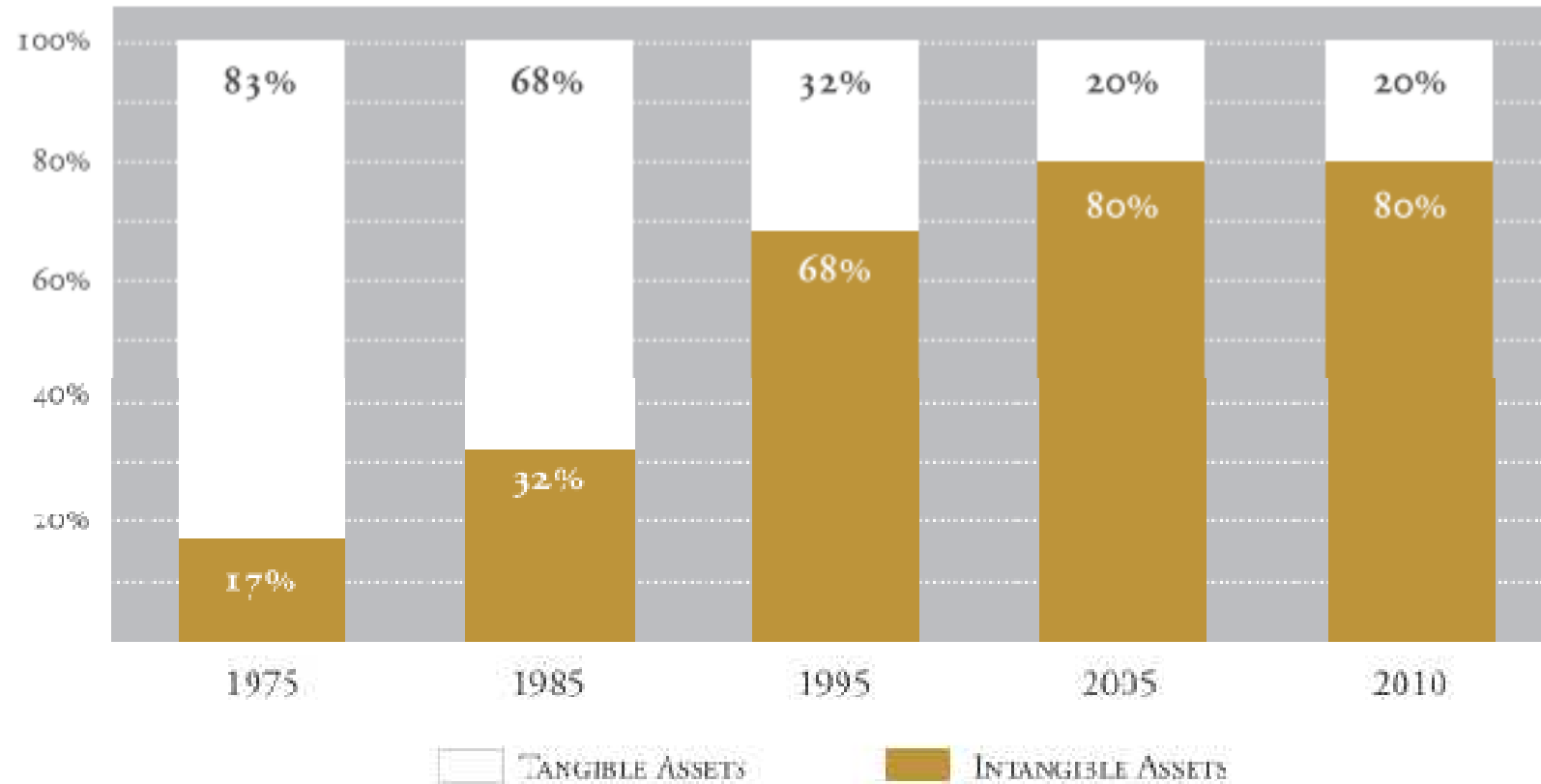
IT Vulnerabilities – The Big 6



Source: Open Source Vulnerability Database

Protecting the Family Jewels

COMPONENTS OF S&P 500 MARKET VALUE

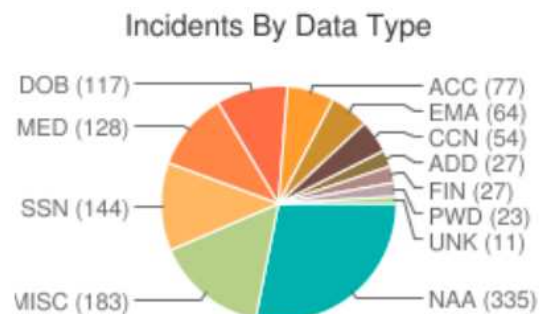
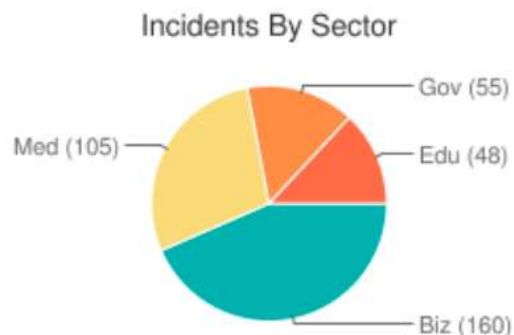


Source: Ocean Tomo

Data Breaches

2011 YTD Data Loss Incidents by Business Type and Data Type

Total Incidents: 369 | Total Records Affected: 126,749,634



Largest Incidents

RECORDS	DATE	ORGANIZATIONS
<u>130,000,000</u>	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
<u>94,000,000</u>	2007-01-17	TJX Companies Inc.
<u>90,000,000</u>	1984-06-01	TRW, Sears Roebuck
<u>77,000,000</u>	2011-04-26	Sony Corporation
<u>40,000,000</u>	2005-06-19	CardSystems, Visa, MasterCard, American Express
<u>35,000,000</u>	2011-07-28	SK Communications, Nate, Cyworld
<u>32,000,000</u>	2009-12-14	RockYou Inc.
<u>26,500,000</u>	2006-05-22	U.S. Department of Veterans Affairs
<u>25,000,000</u>	2007-11-20	HM Revenue and Customs, TNT
<u>24,600,000</u>	2011-05-02	Sony Online Entertainment, Sony Corporation

Latest Incidents

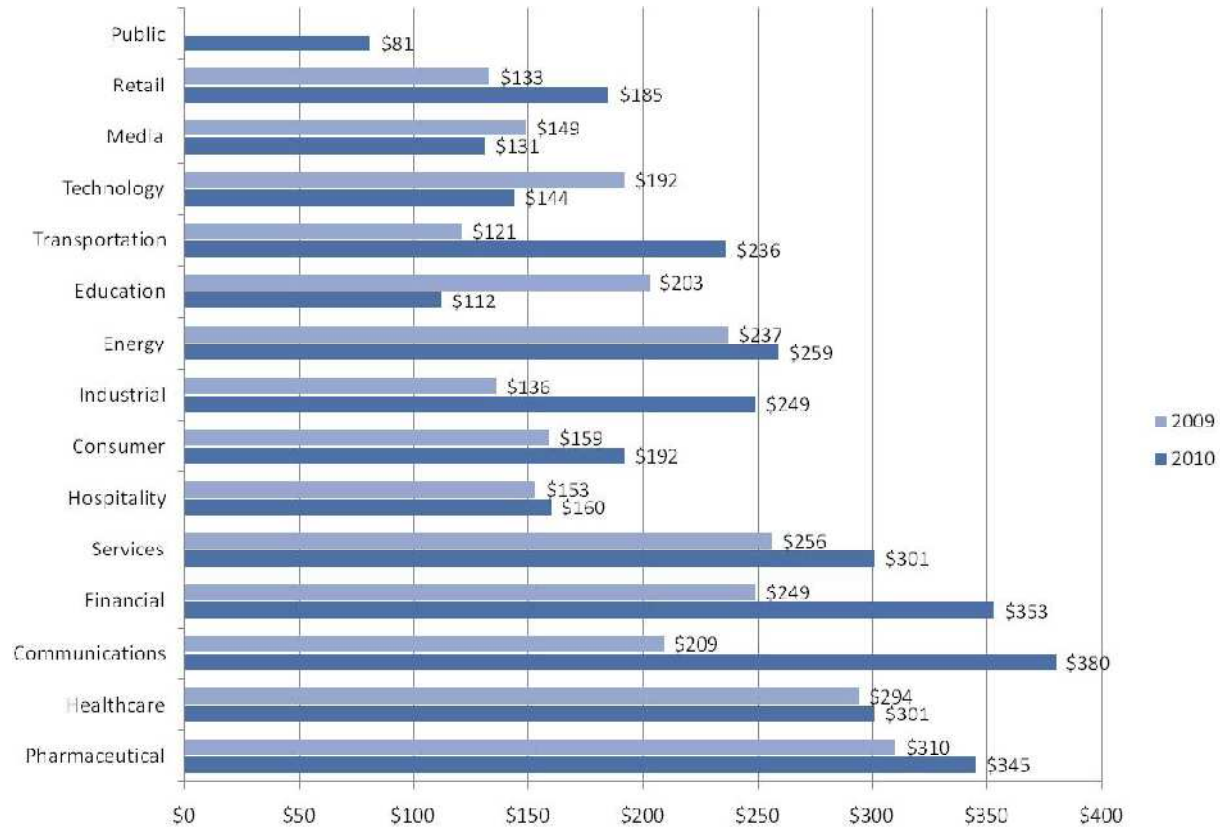
RECORDS	DATE	ORGANIZATIONS
<u>47</u>	2011-11-01	Premier Imaging LLC, High Point Regional Health System, Premier Medical Plaza
<u>5,067</u>	2011-10-31	Hi5ads.com (KathmanduInfosys Educational Consultancy)
<u>1,517</u>	2011-10-31	BanglaTV.ca
<u>0</u>	2011-10-31	British Columbia Ministry of Children and Family Development
<u>30</u>	2011-10-29	Archangel Security Agency Ltd
<u>56</u>	2011-10-28	Hong Kong Labour Department
<u>110</u>	2011-10-28	Unknown Organization, Newcastle Youth Offending Team, Newcastle upon Tyne City Council
<u>593</u>	2011-10-28	United States Air Force
<u>18</u>	2011-10-27	University Hospitals Coventry & Warwickshire NHS Trust
<u>450</u>	2011-10-27	Vancouver Coastal Health Authority

Source: Open Security Foundation Data Loss DB

The Price of Protection?

Cost per Record of Data Breaches by Industry Classification

Avg per Record: \$214 | Avg Organizational Cost per Breach: \$7,241,899



Source: Ponemon Institute

An Ounce of Prevention ...

Preventative Measures Implemented as a Result of a Data Breach

Preventative Measure	2010	2009	2008
Training and awareness programs	63%	67%	53%
Expanded use of encryption	61%	58%	44%
Additional manual procedures and controls	54%	58%	49%
Identity and access management solutions	52%	49%	37%
Data loss prevention (DLP) solutions	43%	42%	26%
Other system control practices	43%	40%	40%
Endpoint security solutions	41%	36%	19%
Security certification or audit	29%	33%	30%
Strengthening of perimeter controls	22%	20%	16%
Security event management systems	21%	22%	21%

Source: Ponemon Institute

The Convergence Challenge?

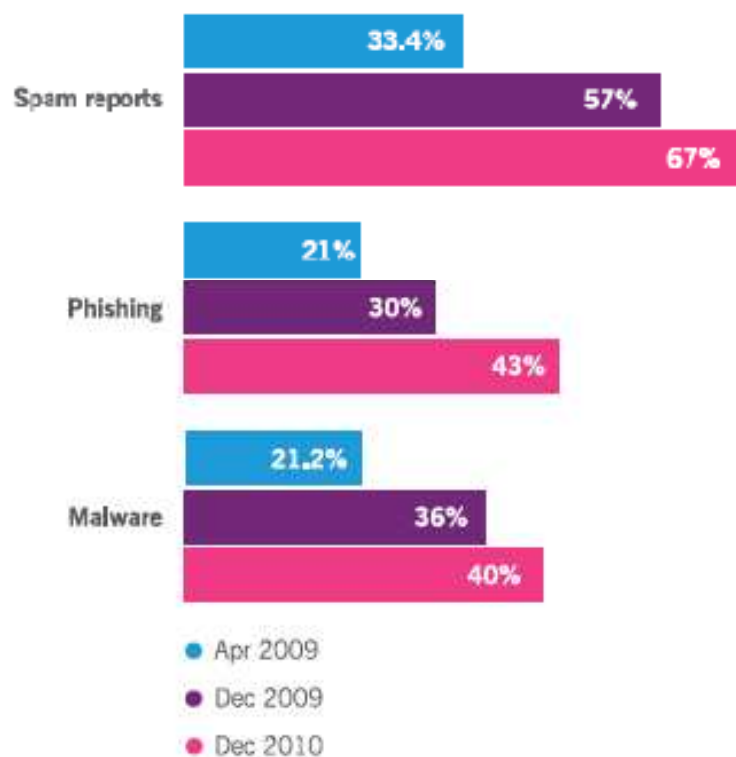
How do we protect information in a universe increasingly dominated by services (Facebook, Google+, Twitter, LinkedIn, etc.) and devices (smartphones, iPads, etc.) designed to make information transparent and portable?



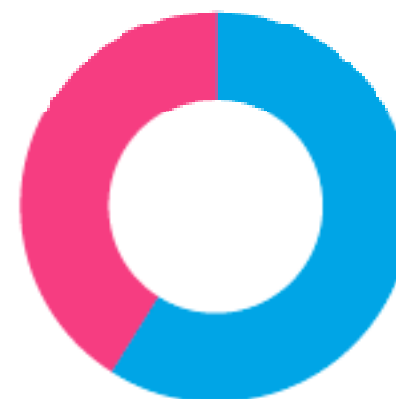
Exposing the Family Secrets



Social network spam, phishing, and malware reports up



Do you think your employees' behavior on social networking sites could endanger security?



● No 41%
● Yes 59%

Source: Sophos

Mobile Divisives?

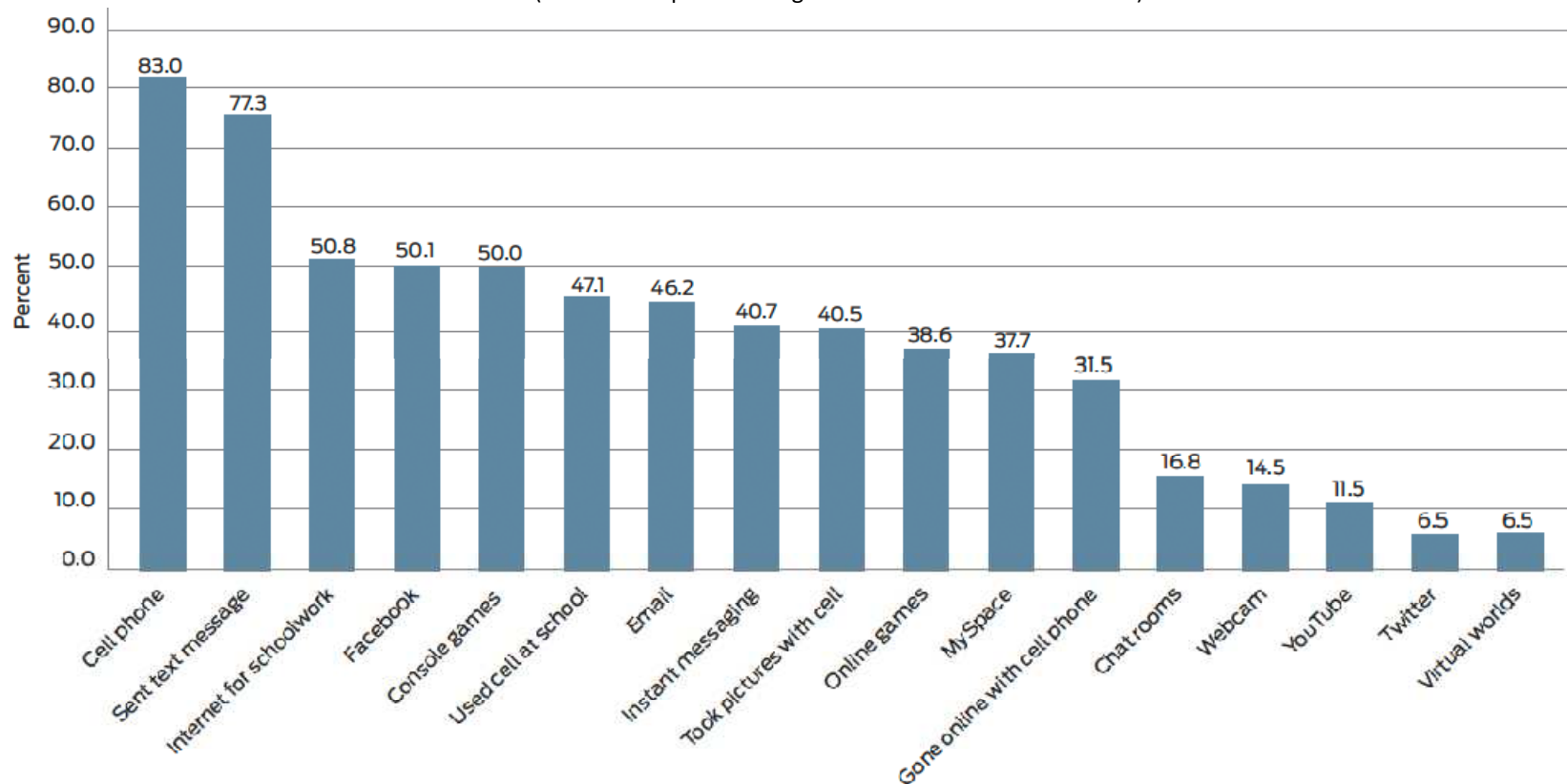
- ~5.3B cell phones worldwide – 8 out of every 10 men, women and children
- 70M cell phones lost each year
- 40% U.S. cell phone users (19% worldwide) have smartphones
- Mobile Web access projected to exceed desktop Web access by 2015
- Social networking apps are 3rd most popular for smartphones
- Only 4% of smartphones have security software installed

A Sobering Thought Re: Mobile

Teens Use of Technology

Weekly Activities of 10- to 18-Year-Olds

n=4441 (random sample from large school district in southern U.S.)

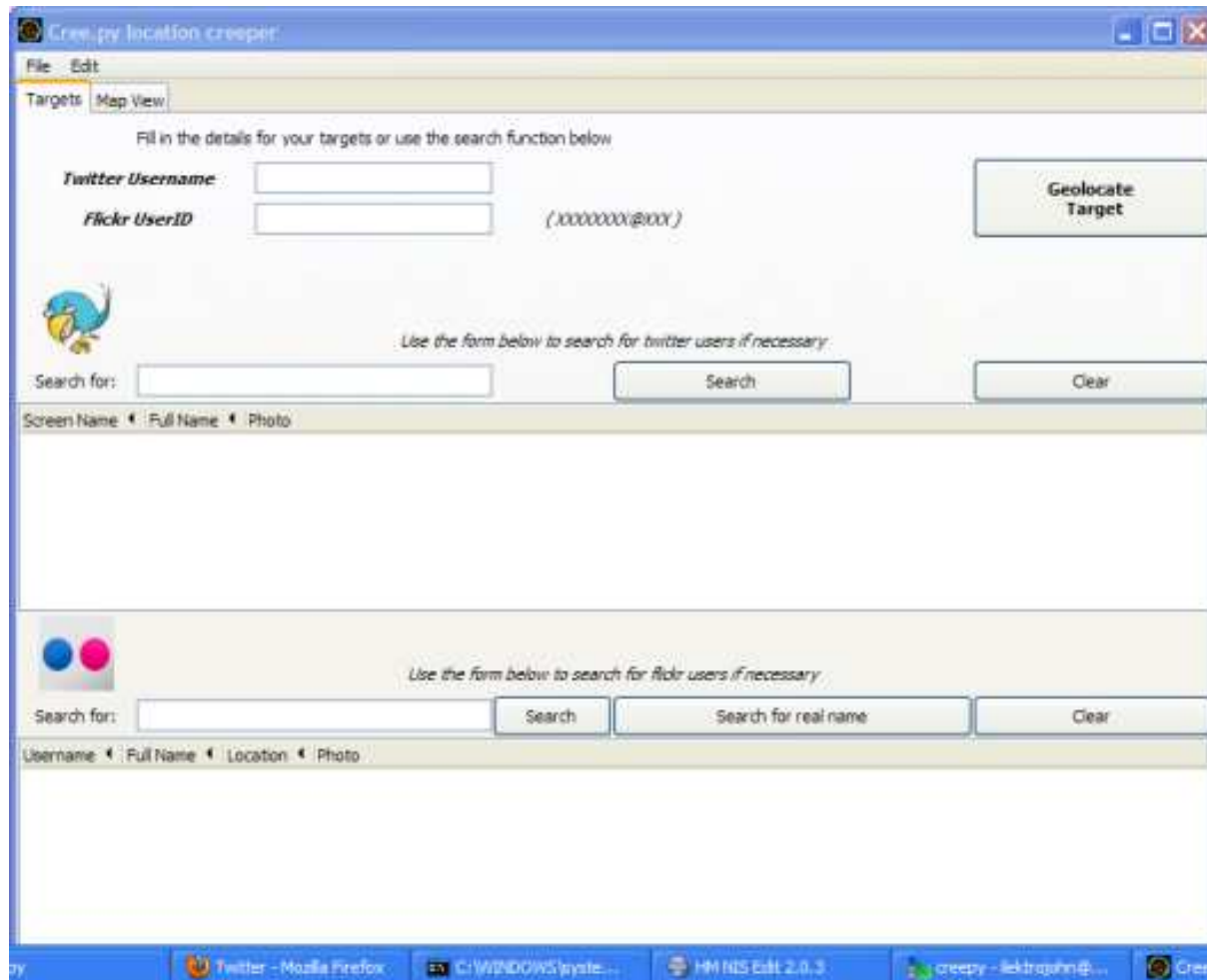


Source: Cyberbullying Research Center

What Next?

- Augmented reality – combining location (GPS) information with social media “friends”
- Digital wallet – very convenient ... for users *and* hackers
- NFC (Near Field Contact) – swipe device to exchange info, transfer \$\$... swap identities?
- Facial recognition – Facebook image tagging already being exploited

Social + Mobile = Creepy



A “Creepy” App

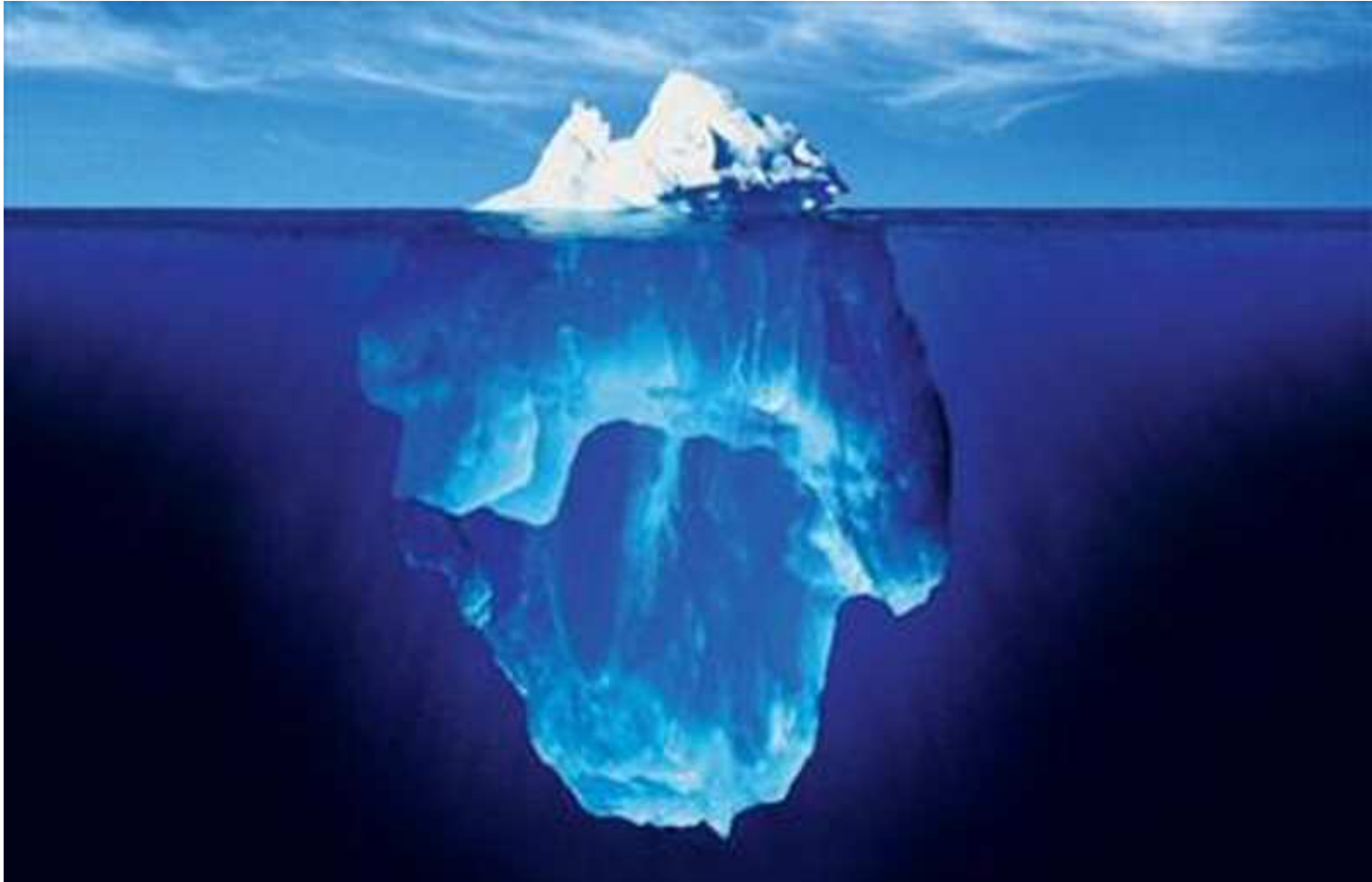
The screenshot shows a window titled "Cree.py location creeper" with a menu bar containing "File" and "Edit". Below the menu bar are two tabs: "Targets" and "Map View". The "Targets" tab is active, displaying a table with the following data:

Latitude	Longitude	Time
59.858393	17.637691	2010-08-30 23:25:08
59.858393	17.637691	2010-08-30 23:25:00
59.858393	17.637691	2010-08-30 23:24:43
59.858393	17.637691	2010-08-30 23:24:34
59.858393	17.637691	2010-08-30 23:24:26
59.858393	17.637691	2010-08-30 23:24:15
59.858393	17.637691	2010-08-30 23:24:08
59.858393	17.637691	2010-08-30 23:23:59
59.858393	17.637691	2010-08-30 23:23:52
59.858393	17.637691	2010-08-30 23:23:46
59.858393	17.637691	2010-08-30 23:23:39
59.858393	17.637691	2010-08-30 23:23:26
59.858393	17.637691	2010-08-30 23:23:19
59.858393	17.637691	2010-08-30 23:23:12
59.858393	17.637691	2010-08-30 23:23:04
59.858393	17.637691	2010-08-30 23:22:57
59.858393	17.637691	2010-08-30 23:22:48
59.858393	17.637691	2010-08-30 23:22:38
59.858393	17.637691	2010-08-30 23:22:31
59.858393	17.637691	2010-08-30 23:22:21
59.858393	17.637691	2010-08-30 23:22:11

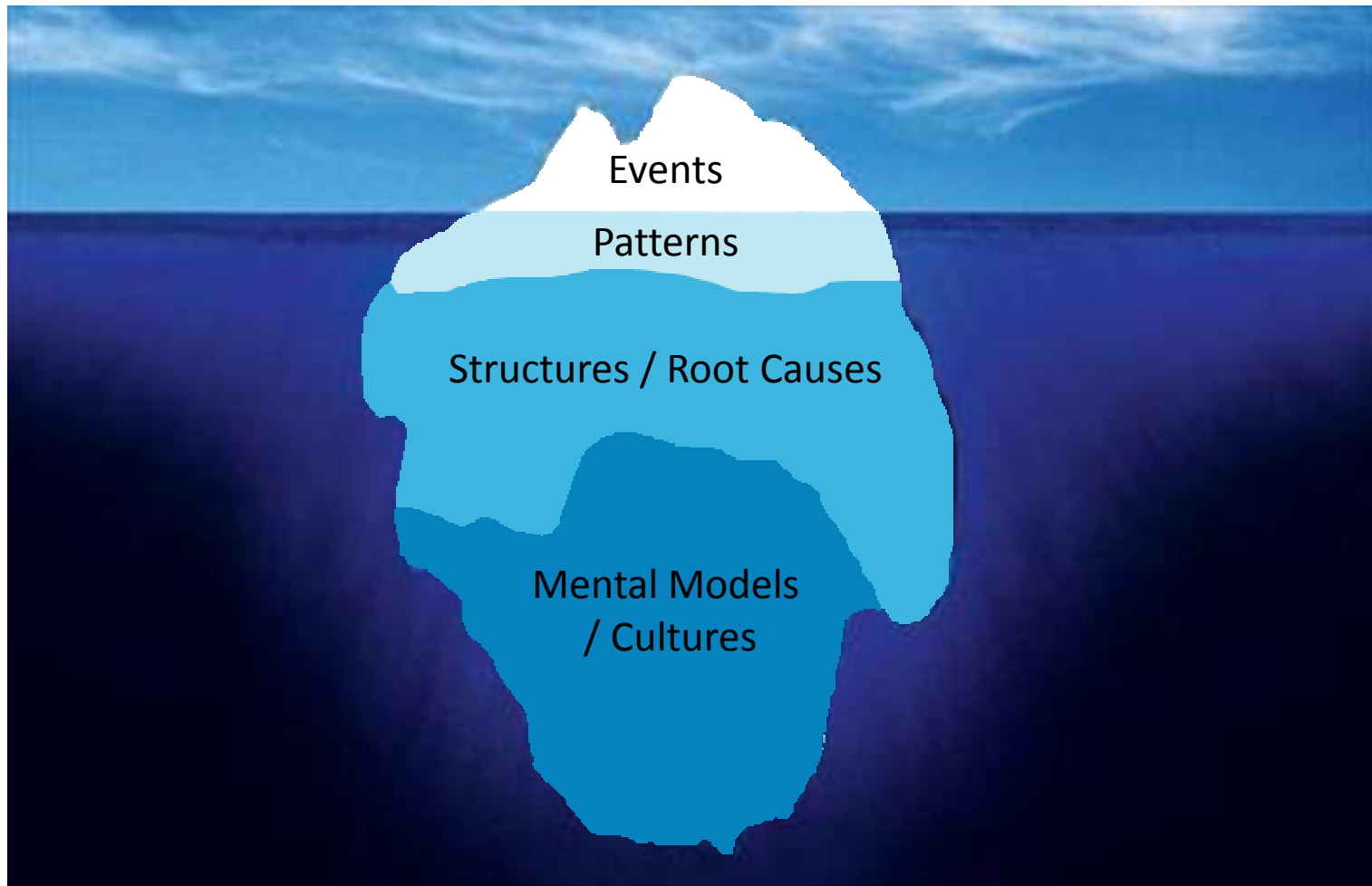
The "Map View" tab shows a satellite map of Uppsala, Sweden. A red location pin is placed on the map, corresponding to the coordinates in the table. The map includes a scale bar (200m / 300yd) and coordinates (N 59° 51' 50", E 017° 38' 26"). Below the map, there is a text box with the following information:

Photo from flickr
Title : Uppsala domkyrka
<http://www.flickr.com/photos/43529418@N06/4943217596>

This Might Be the Only Secure Place To Be



The Iceberg Model Redux



About Me



What now?

- William.Ender@EMC.com
- twitter.com/GRCevangelist
- Read Yo Delmar! – yogrc.typepad.com (*GRC and Beyond* blog)

Final Thought

“If you want total security, go to prison ... The only thing lacking is freedom.”

– Dwight D. Eisenhower