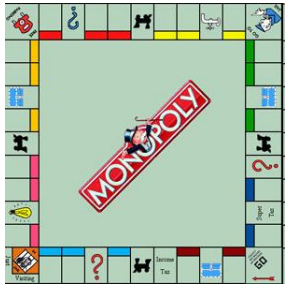
A game of information security

Monopoly or Stratego

Dr Theodoros Stergiou, CEng, CPMM,
Security Solutions Product Manager

Monopoly or Stratego

- Monopoly
  - Market domination by a single entity
  - To win, all other users need to go bankrupt
  - Strategy is involved; visibility into opponent's moves



- Stratego
  - Capture the flag
  - A game of disinformation, discovery and psychology
  - A purely strategic game; no visibility into opponent's moves

State of vulnerabilities

Table 7. Top 10 Threat Action Types by number of breaches and records

Rank	Variety	Category	Breaches	Records
1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	48%	35%
2	Exploitation of default or guessable credentials	Hacking	44%	1%
3	Use of stolen login credentials	Hacking	32%	82%
4	Send data to external site/entity	Malware	30%	<1%
5	Brute force and dictionary attacks	Hacking	23%	<1%
6	Backdoor (allows remote access/control)	Malware	20%	49%
7	Exploitation of backdoor or command and control channel	Hacking	20%	49%
8	Disable or interfere with security controls	Malware	18%	<1%
9	Tampering	Physical	10%	<1%
10	Exploitation of insufficient authentication (e.g. no login required)	Hacking	5%	<1%

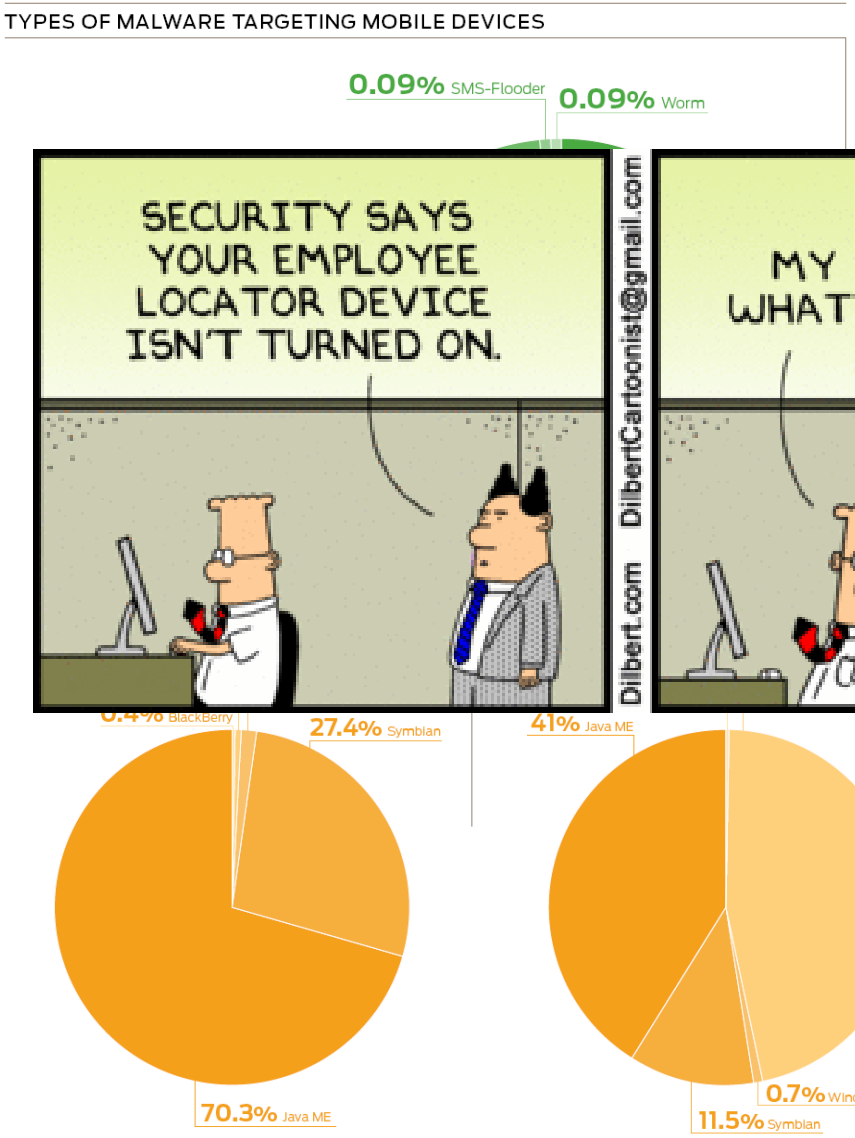
** Verizon 2012, Data breach investigations report*

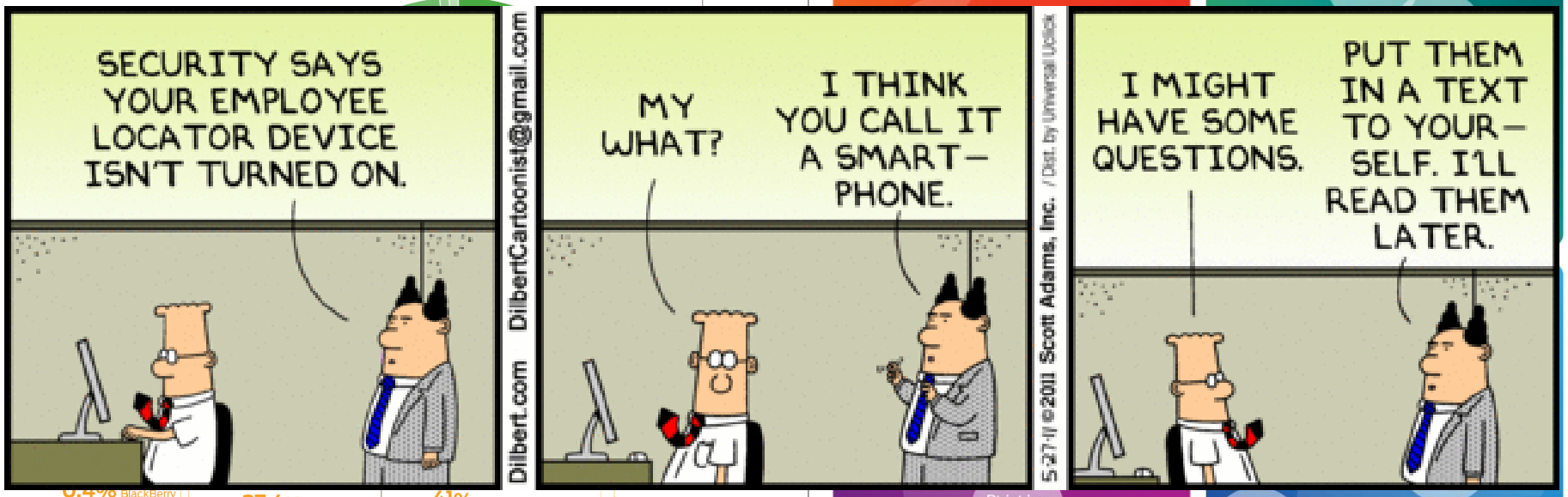
State of breaches

Publicized	Target	Alleged Source/Motive	Method	Harm
2/5/11	Sony Online Entertainment	unknown	Unknown	Information for about 24.6 million customers, including names, addresses, e-mail addresses, gender, birth dates, phone numbers, log-in names, and hashed passwords may have been stolen. Also, credit and debit card numbers and expiration dates for about 12,700 non-U.S. customers from an "outdated" database and about 10,700 direct debit records listing bank account numbers of customers in Germany, Austria, the Netherlands, and Spain may have been stolen.
2/6/11	Sony Pictures	LulzSec	SQL Injection	Personally identifying information of 37,500 customers was exposed, including address, e-mail address, phone number, date of birth, password and user name.
4/7/11	Apple	AntiSec	exploited security flaw in the software Apple used	26 admin usernames and passwords for an Apple server exposed
11/2/11	HBGary Federal	Anonymous hacks Web site, Twitter and LinkedIn accounts of firm that was investigating its members	unknown	e-mails and other sensitive data leaked online
2/2/12	VeriSign	unknown	unknown	Hackers broke into corporate servers and stole information in several attacks in 2010, the company revealed in an SEC filing in October 2011. The company did not say what data was stolen.
3/2/12	Greece's Justice Ministry	Anonymous protesting against Greece's bailout by the EU and the IMF, which led to austerity measures.	unknown	unclear
8/2/12	Symantec	Hackers believed affiliated with Anonymous	unknown	Hackers stole source code from Symantec in 2006 and released it this week on the Web after allegedly trying to extort $50,000 from Symantec.
12/25/2011	Stratfor	LulzSec, AntiSec	unknown	860,000 e-mail addresses, 75,000 unencrypted credit card numbers stolen and later released publicly
3/17/2011	RSA	unknown attacker, although China believed to be suspect. Motive is probably espionage	Advanced Persistent Threat (APT) targeted at individuals within an organization using social engineering. Malware hidden in an Excel spreadsheet exploited a zero-day (unpatched) Flash hole.	SecurID token deployments at financial, government and other sites were at risk.

** cnet, 2012*

New concerns – mobility

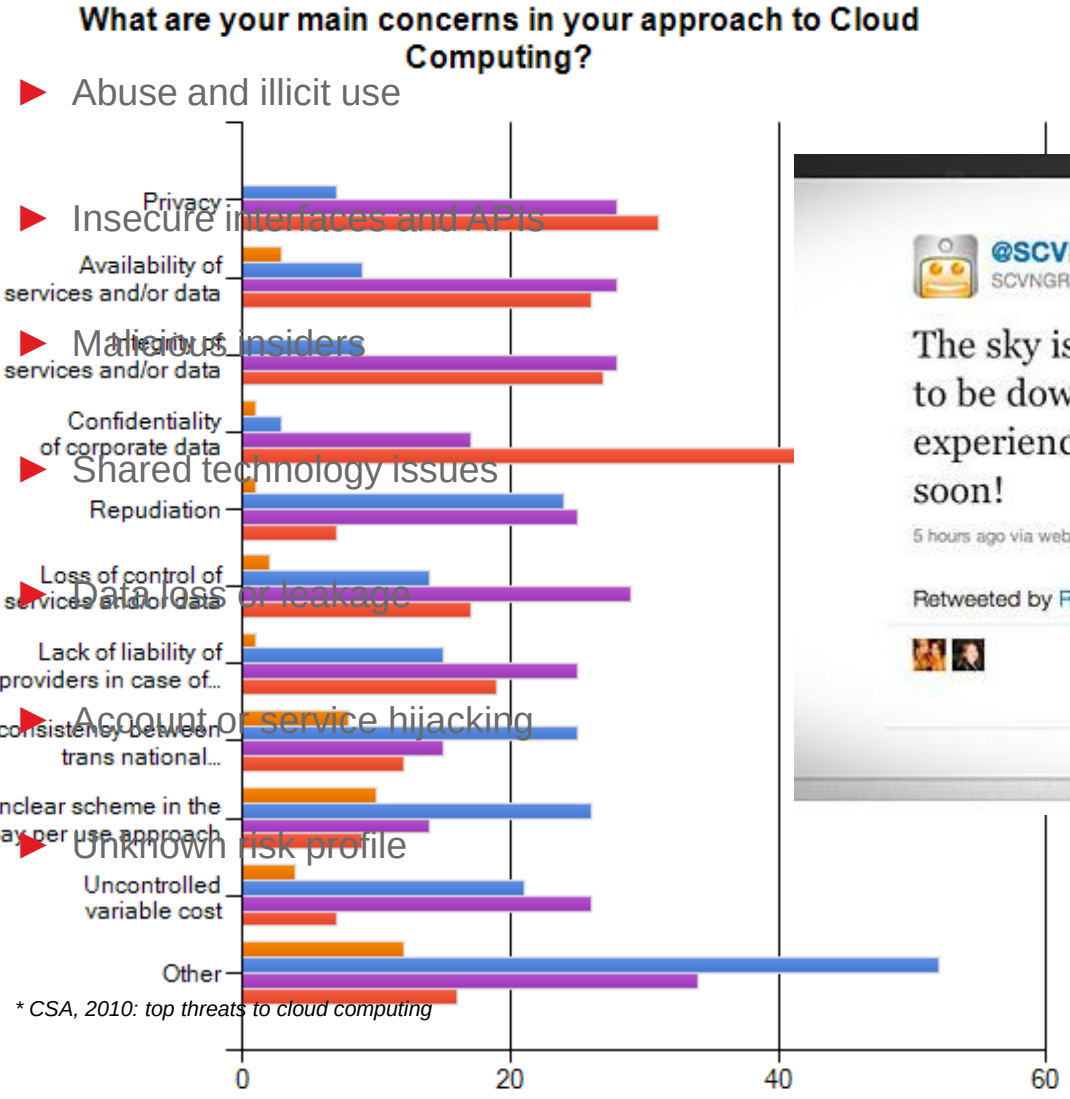




** CISCO, 2010 annual security report*

** Juniper, 2011 mobile threats report*

New concerns – cloud



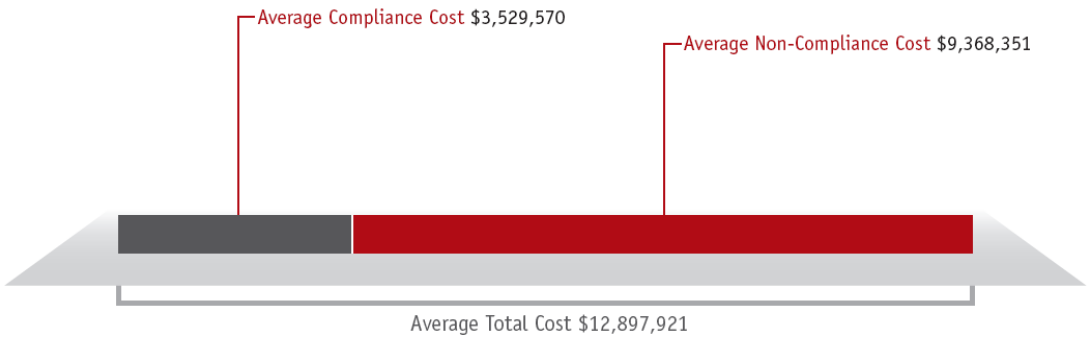
** CSA, 2010: top threats to cloud computing*

- Abuse and illicit use
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

** ENISA: Survey on An SME perspective on Cloud Computing, Nov 2009*

Increased concerns – compliance

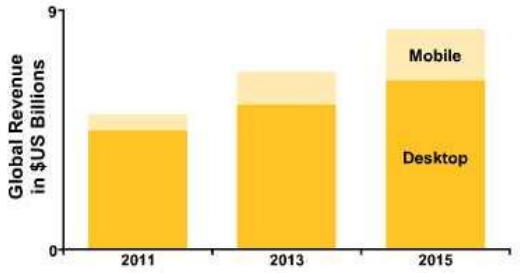
- Complying to regulations is still regarded as a business burden
- Compliance is not though fully understood
  - It is not about checkboxes
  - It is not about fines and penalties
  - It is about building up a mentality, a culture of security
- On an effort scale
  - The more effective a security strategy is, the lower the cost of non-compliance
  - Laws and regulations are the main drivers for such investment



** Ponemon Institute, 2011: "The true cost of compliance"*

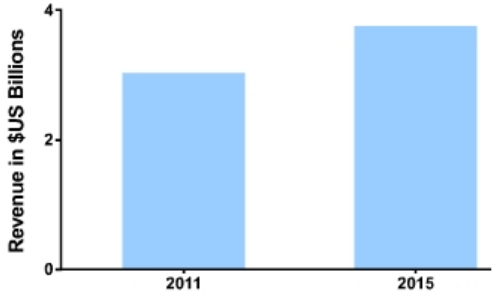
The market in numbers

Client security market is forecast to hit $8.2 billion in 2015, fueled by growth in mobile clients



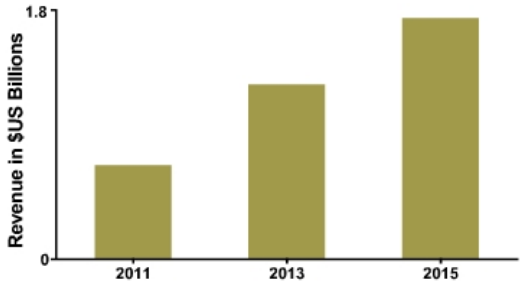
© Infonetics Research, *Security Client Software Biannual Market Size, Share, and Forecasts*, October 2011

The global content security appliances and software market is forecast to reach $3.7 billion in 2015

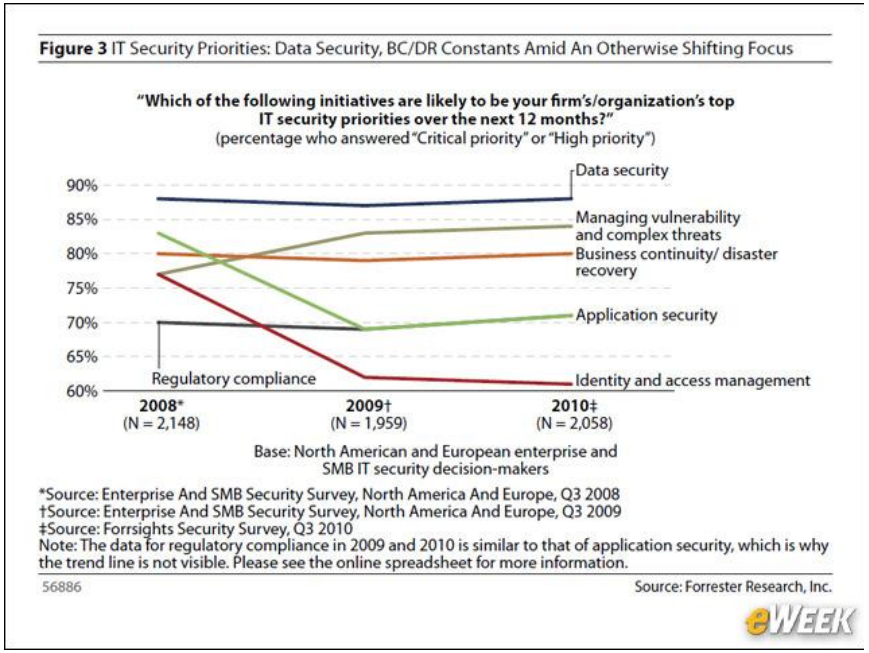


© Infonetics Research, *Content Security Appliances and Software Quarterly Market Share, Size, and Forecasts*, Nov. 2011

Global spending on virtual security appliances is forecast to hit $1.7 billion in 2015



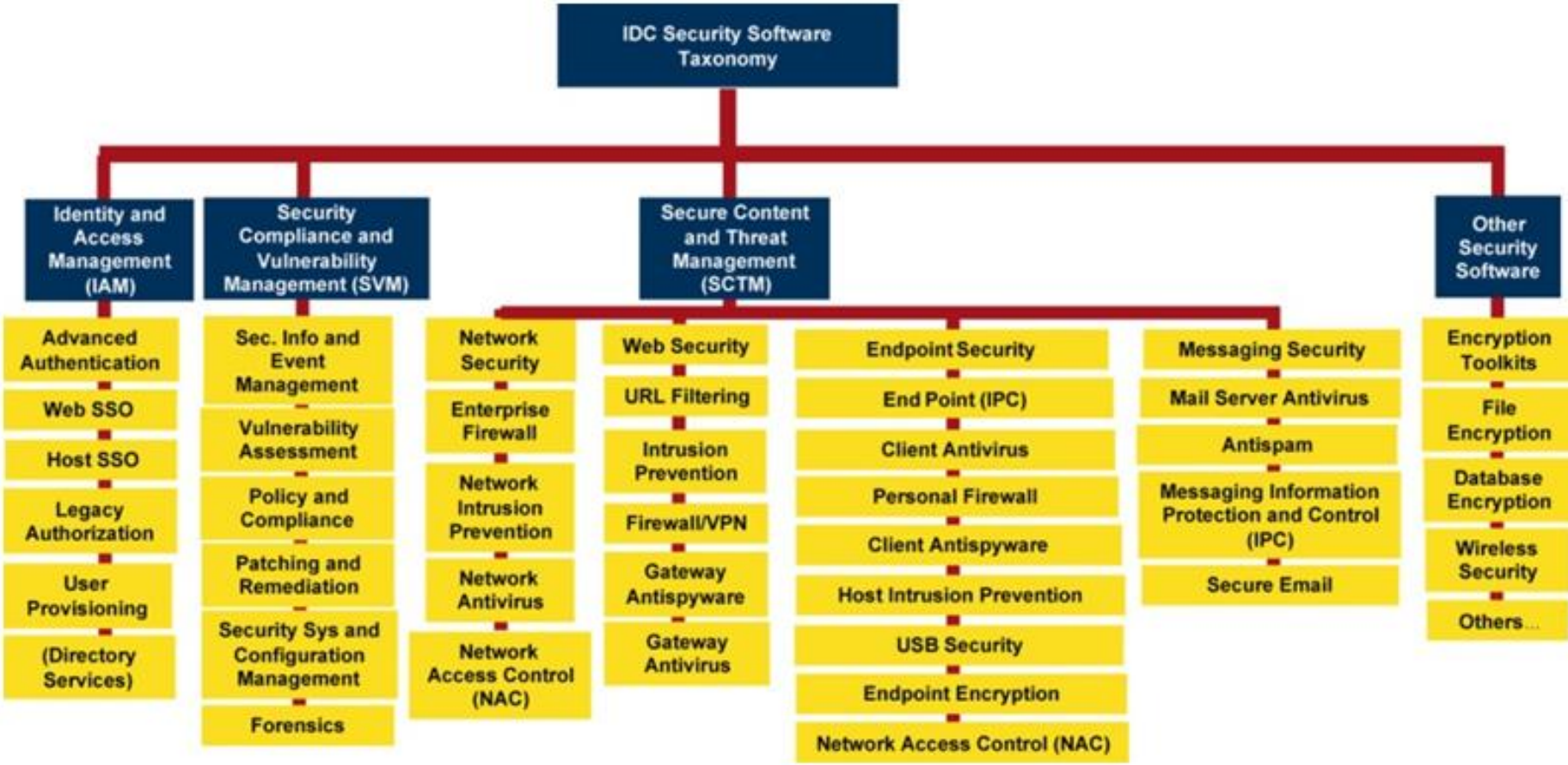
© Infonetics Research, *Virtual Security Appliances Biannual Market Size and Forecasts*, Dec. 2011



The market, says **Gartner** in its report – Forecast: Security Service Market, Worldwide, 2011 – is estimated at $38.3 billion in 2012, and is likely to surpass the $49.1 billion mark in 2015.

The global network security appliance and software market grew 8% in 4Q11 to $1.58 billion (Infonetics, 2012)

So many cards to pick – just like Monopoly



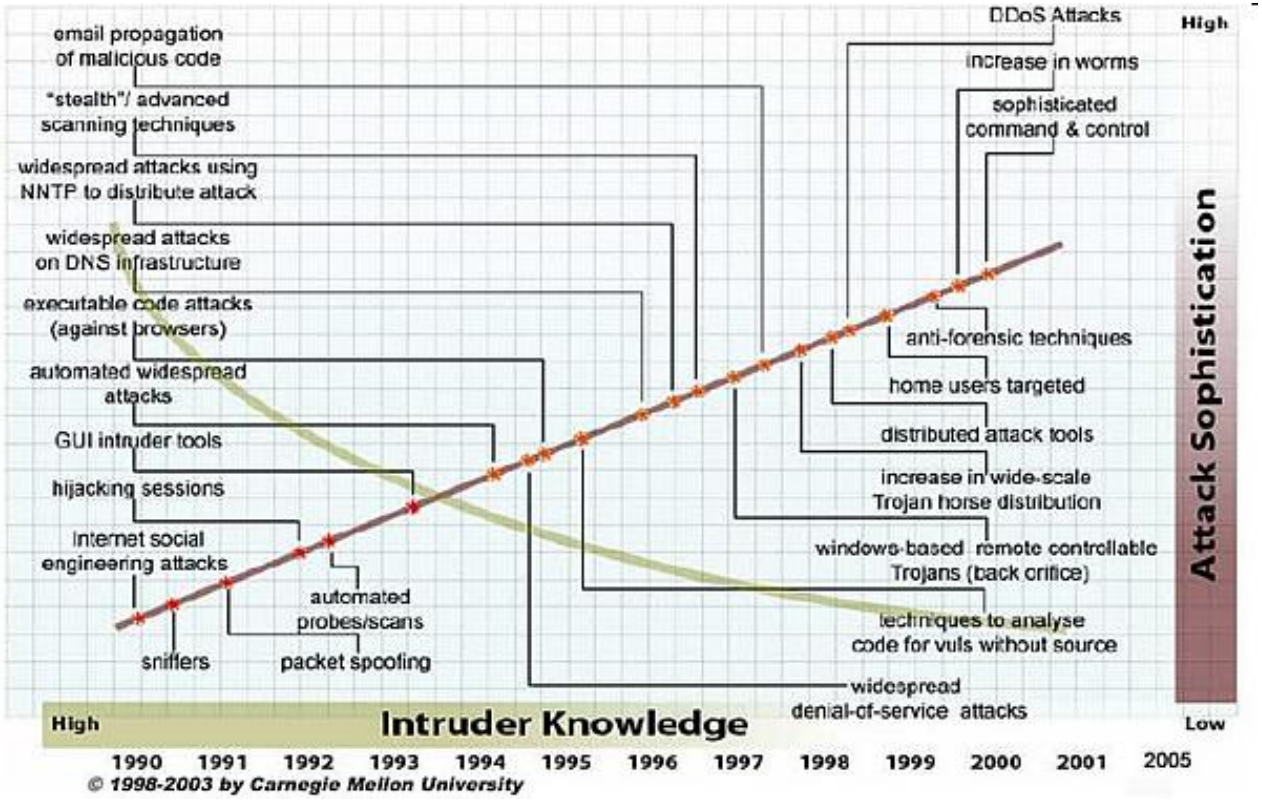
Attackers playing Stratego

WHO IS BEHIND DATA BREACHES?

- **98%** stemmed from external agents (+6%)
- **4%** implicated internal employees (-13%)
- **<1%** committed by business partners (↔)
- **58%** of all data theft tied to activist groups

HOW DO BREACHES OCCUR?

- **81%** utilized some form of hacking (+31%)
- **69%** incorporated malware (+20%)
- **10%** involved physical attacks (-19%)
- **7%** employed social tactics (-4%)
- **5%** resulted from privilege misuse (-12%)



** Verizon 2012, Data breach investigations report*

Do we understand the challenges?

- Still several companies struggle to identify real needs
  - E.g. data loss vs. data leakage
- Identifying budget really required on security
- Define what we mean by security and what kind of security we really want
- Educate employees/users
- Say no to hypes and trends
- Our problem is not DDoS – our problem is **Denial of Mistakes***

** Brian Goldman, TED Conference, 2011: "Doctors make mistakes, can we talk about that?"*

Conclusions

- Organizations must play both games
  - Obtain security solutions using a specific strategy, not because of a trend
  - Monitor & observe concealing playing cards

- Realize that security does not produce RoI but **Return on Value (RoV)**

Our company


IS Service Offerings
Strategy Services
Policy & Standards Development
Compliance Assessment
Operations Support
Engineering Services
Architecture Design & Implementation
Systems Health Assessment
Awareness & Optimization
Application Security Solutions
Web Application Firewall
Web Content Security
E-mail Security
Single Sign On (SSO)
IS Service & Solution Offerings
System Security Solutions
Endpoint Security
UC & VoIP Security
Security Management & Monitoring
Security Incident & Event Management
Network Security Solutions
DDoS Mitigation
Network Admission Control
Network Perimeter Security
IS Solution Offerings

thank you

sitronics
telecom solutions

INTRACOM
TELECOM

www.intracom-telecom.com