Today's Security Threats Uncovered

Symantec Internet Security Threat Report

Brian J. Tillett

Chief Security Strategist
Symantec Public Sector

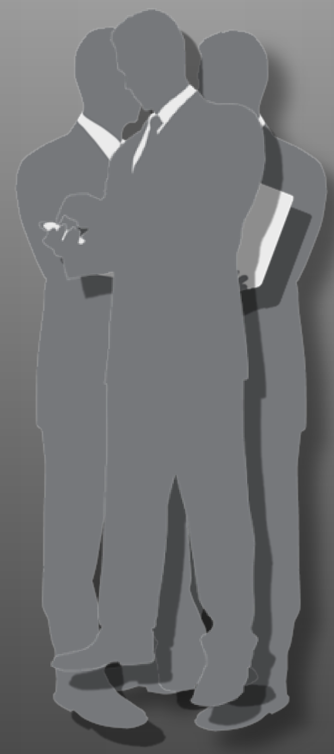

KEY TRENDS
CONSUMERIZATION
IT-IFICATION
MOBILE
SOCIAL
VIRTUALIZATION
CLOUD
DATA GROWTH
THREAT LANDSCAPE
Symantec.

Employees Connect In A Whole New Way

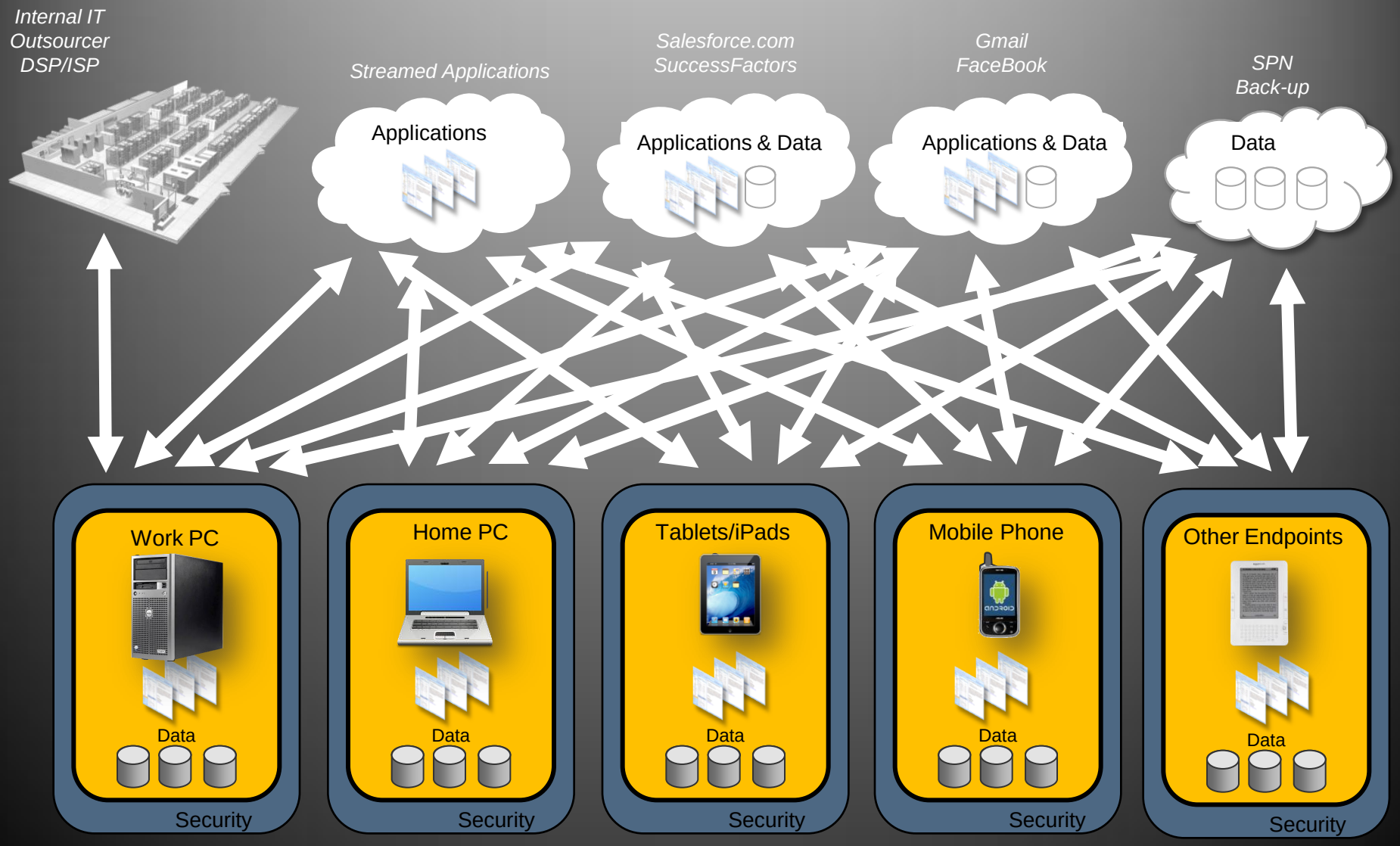
Edits ROI models with his team on Office Live.

Downloads the latest presentation from SharePoint.

Updates status on his Facebook profile.



What does this all mean for IT Security?



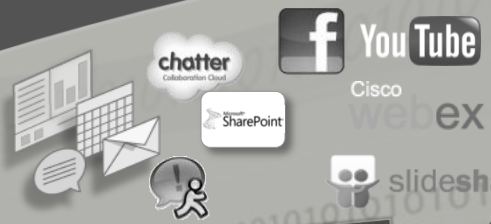
Symantec

IT Must Evolve to Meet New Demands

System-Centric

- Driver: Business automation, e.g., ERP, functional apps
- Data: Centralized, structured
- Infrastructure: Physical
- IT focus: Systems tasks

Information-Centric



- Driver: Next level of productivity and agility with collaboration and knowledge sharing
- Data: Distributed, unstructured
- Infrastructure: Virtual, cloud, outsourced

Symantec Global Intelligence Network

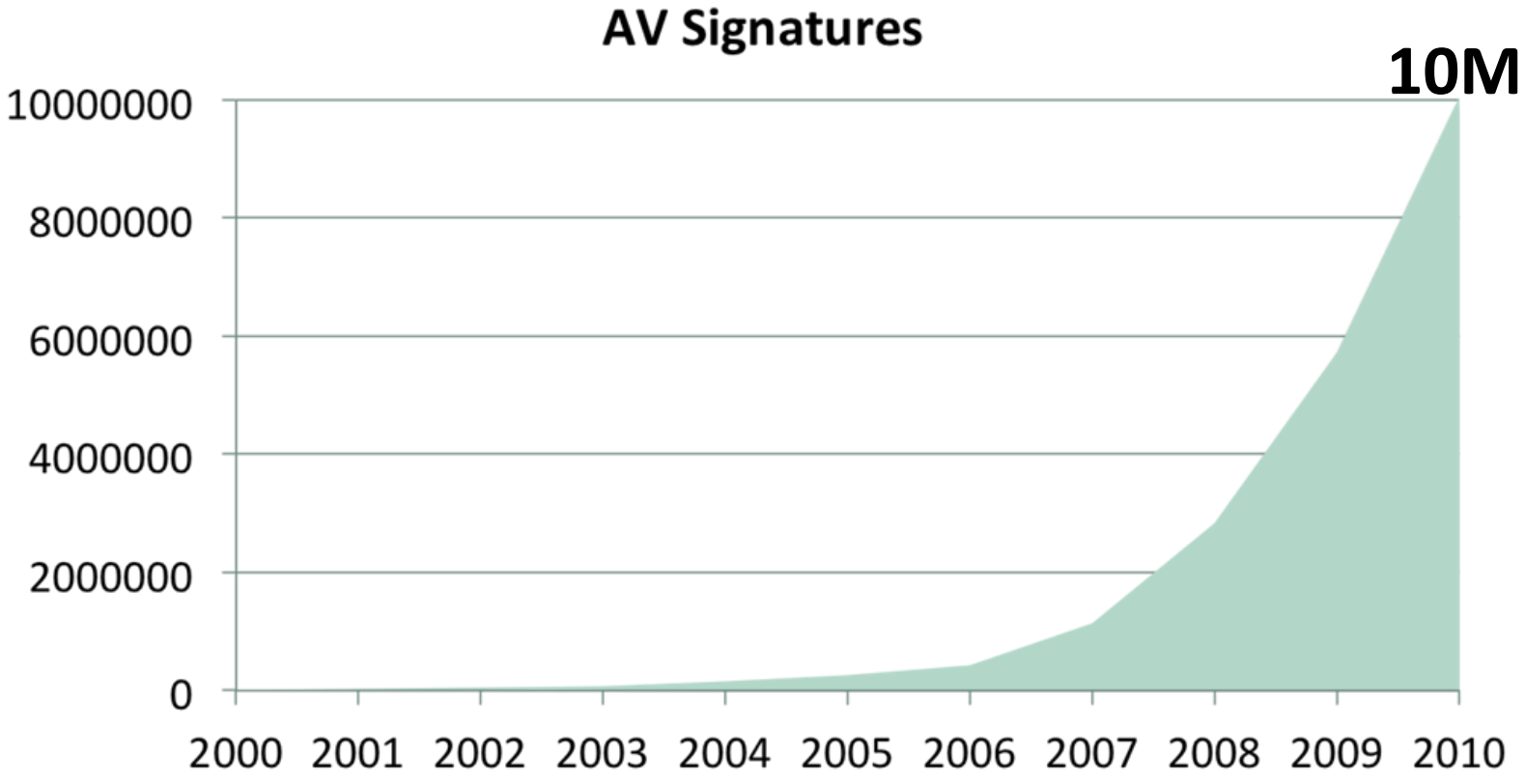
Worldwide Coverage | **Global Scope and Scale** | *24x7 Event Logging*

Rapid Detection

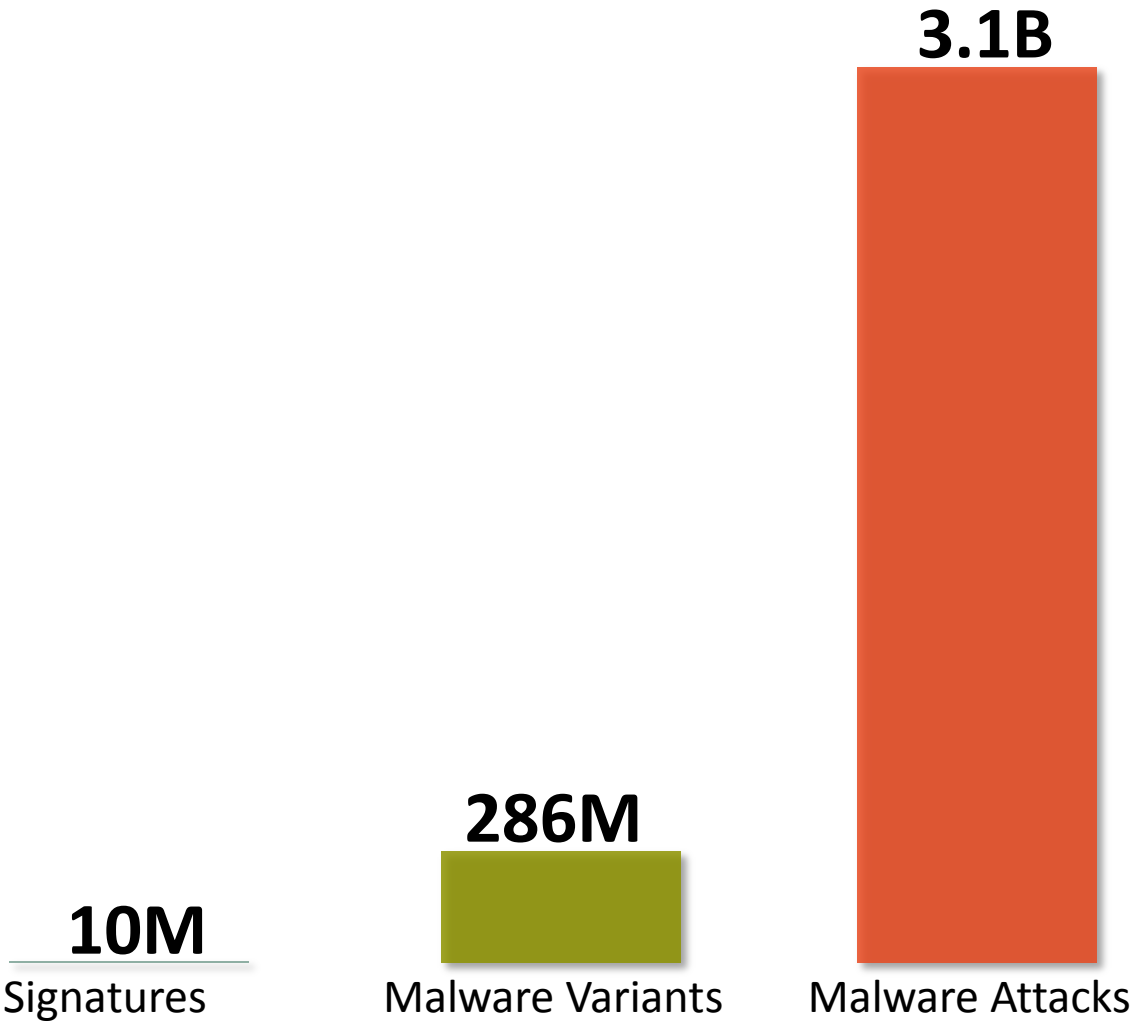
Attack Activity	Malware Intelligence	Vulnerabilities	Spam/Phishing
• 240,000 sensors • 200+ countries & territories	• 175M client, server, gateways monitored • Global coverage	• 40,000+ vulnerabilities • 14,000 vendors • 105,000 technologies	• 5M decoy accounts • 8B+ email messages/day • 1B+ web requests/day

Preemptive Security Alerts | **Information Protection** | *Threat Triggered Actions*

AV Signatures in Perspective



AV Signatures in Perspective



Threat Landscape

2010 Trends

1. **Targeted Attacks**
   continued to evolve

2. **Social Networking**
   + social engineering = compromise

3. **Hide and Seek**
   (zero-day vulnerabilities and rootkits)

4. **Attack Kits**
   get a caffeine boost

5. **Mobile Threats**
   increase

❶ Targeted attacks continue to evolve

- High profile targeted attacks in 2010 – Hydraq and Stuxnet – raised awareness of the consequences of APTs

January

1 **Trojan.Hydraq**

News breaks of a high-profile targeted threat affecting multinational corporations around the globe.

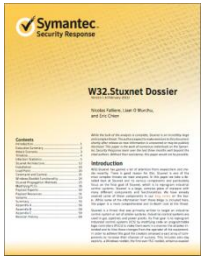
June

17 **Stuxnet**

The first reports of a new threat leveraging a zero-day vulnerability. This threat would go on to become one of the biggest malware events of the year.

- Stuxnet signaled a leap in the sophistication of these types of attacks
  - Four zero-day vulnerabilities
  - Stolen digital signatures
  - Ability to "leap" the air gap
  - Potential damage to infrastructure

More Info:



Detailed review in the: *W32.Stuxnet Dossier* & *W32.Stuxnet*

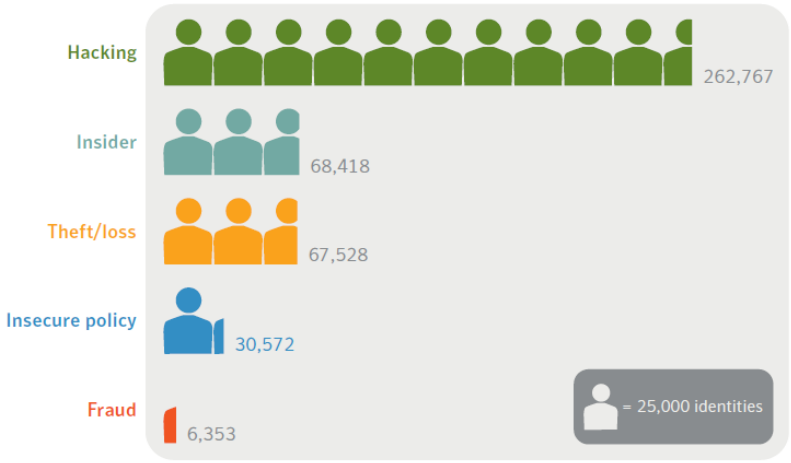
❶ Targeted attacks continue to evolve

- Less sophisticated attacks also cause significant damage

260,000

Identities Exposed per Breach

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.



Average Number of Identities Exposed per Data Breach by Cause

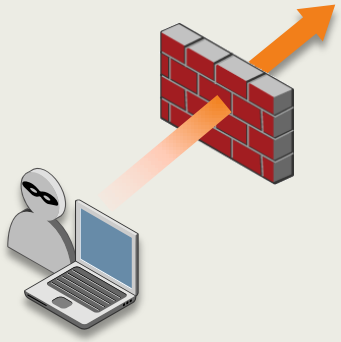
- The average cost to resolve a data breach in 2010 was $7.2 million USD.

Threat Landscape

❶ Targeted attacks

How it works: APT Advanced Persistent Threat

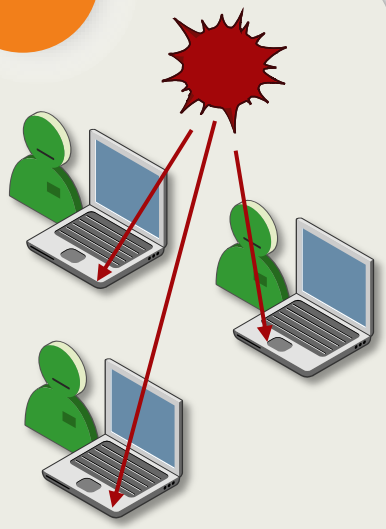
1



INCURSION

Attacker breaks into the network by delivering targeting malware to vulnerable systems and employees

2

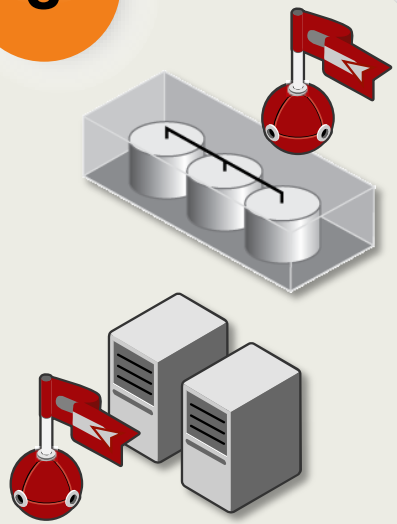


DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

3

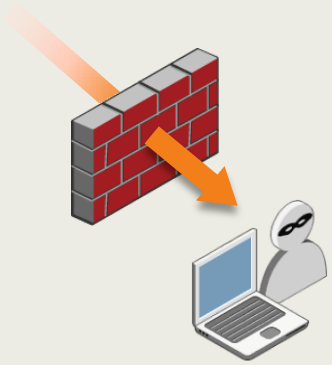


CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire data or disrupt operations

4



EXFILTRATION

Data sent to back to enemy's "home base" for exploitation/fraud

Disruption of operations or destruction of equipment


STUXNET

Stuxnet milestones in malicious code history:

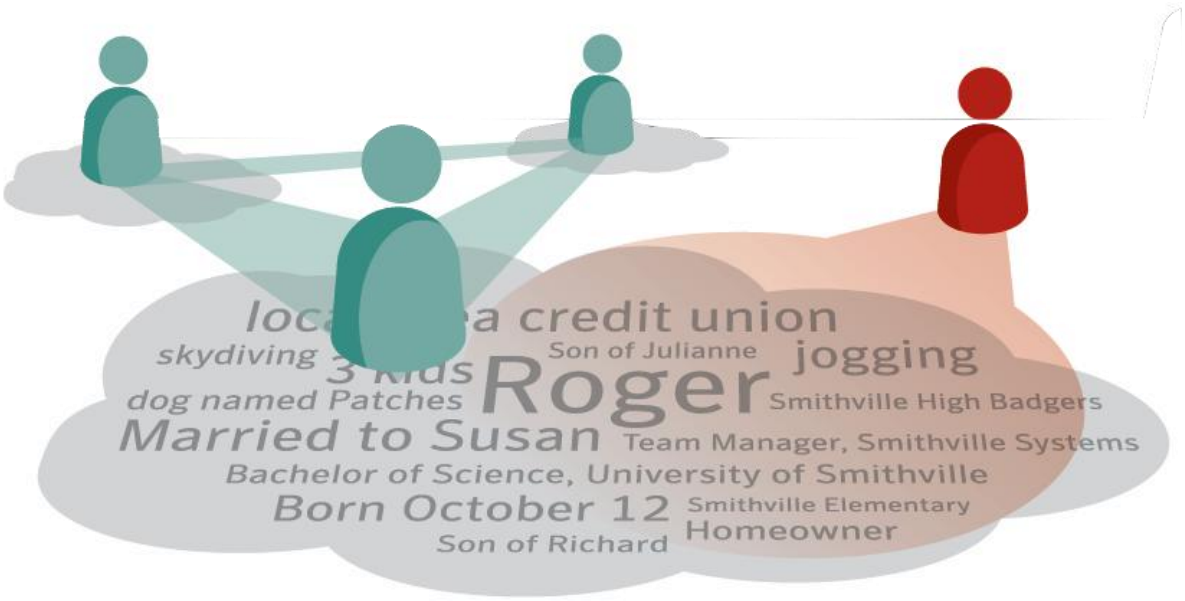
	Typical Malware	Stuxnet
0-Day vulnerabilities	None	4
Little known vulnerabilities	None	2
Propagation methods	1 - 2	7
Attack self-contained	No, always downloads more malware	**Yes, all inclusive package; encrypted**
Stolen Digital Signatures	Never; rare faked or expired signature	2

…AND IT JUMPED AIR-GAPPED NETWORKS!

Duqu Trojan aka *Stuxnet 2.0, October 2011*

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	XXXXX
Injection based on A/V list	✓	✓ seems based on Stu
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?

❷ Social networking + social engineering = compromise



More Info:

Detailed review of Social Media threats available in *The Risks of Social Networking*

- Hackers have adopted social networking
  - Use profile information to create targeted social engineering
  - Impersonate friends to launch attacks
  - Leverage news feeds to spread SPAM, scams and massive attacks

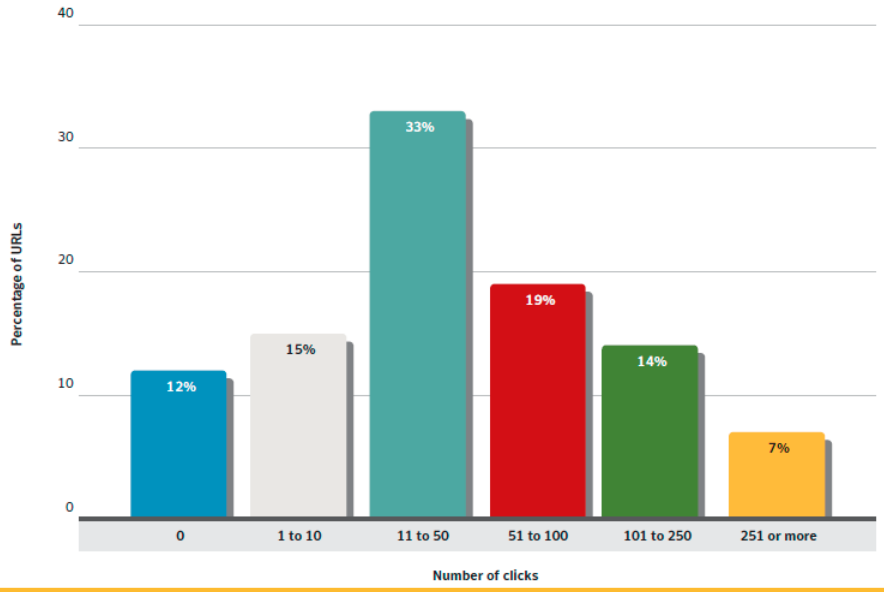
❷ Social networking + social engineering = compromise

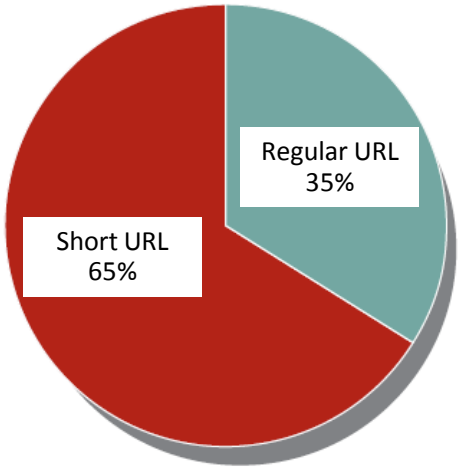
- Shortened URLs hide malicious links, increasing infections

Regular URL http://en.wikipedia.org/wiki/URL_shortening

Shortened URL http://goo.gl/Hsxsn

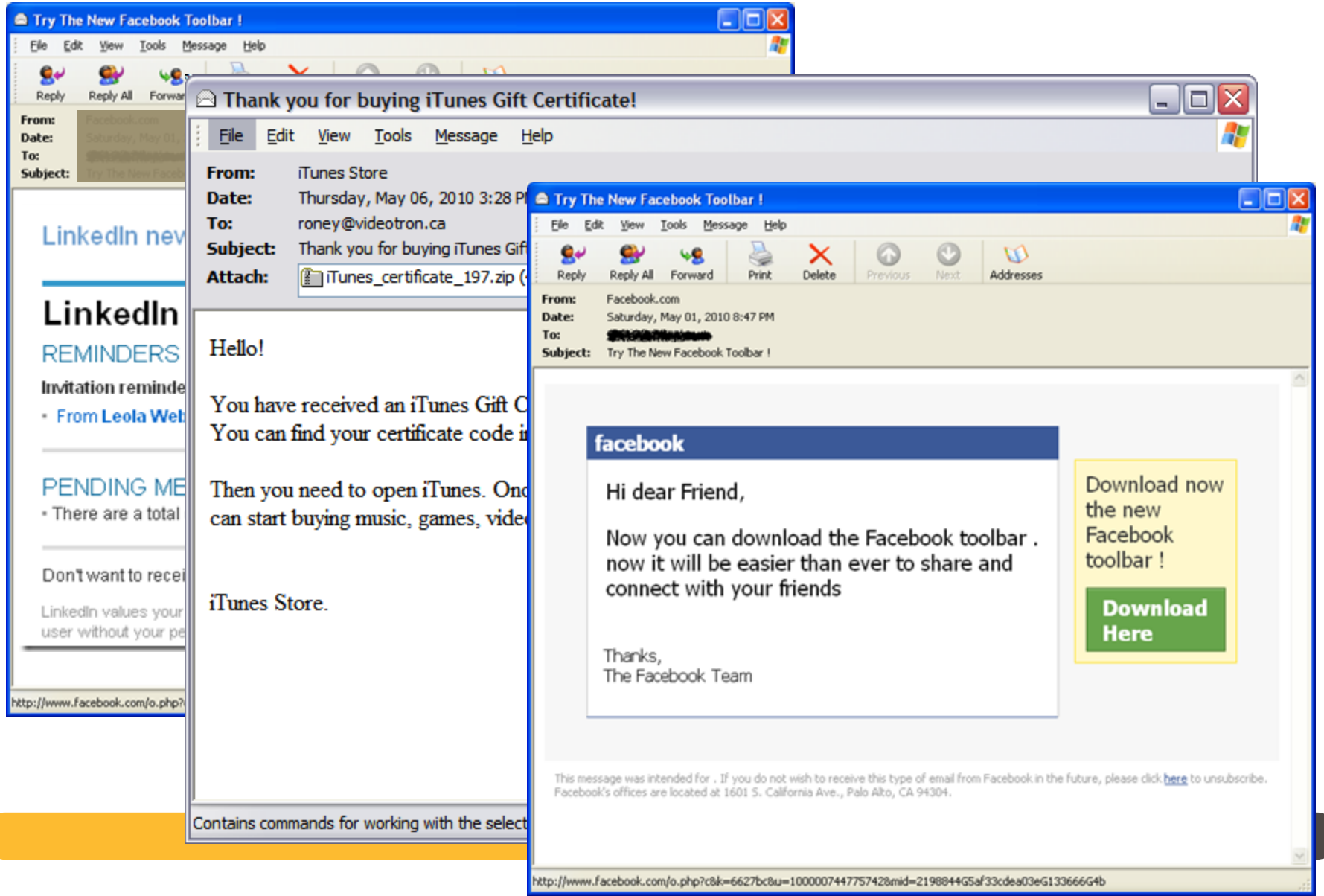
- Shortened URLS leading to malicious websites observed on social networking sites, 73% were clicked 11 times or more





Threat Landscape

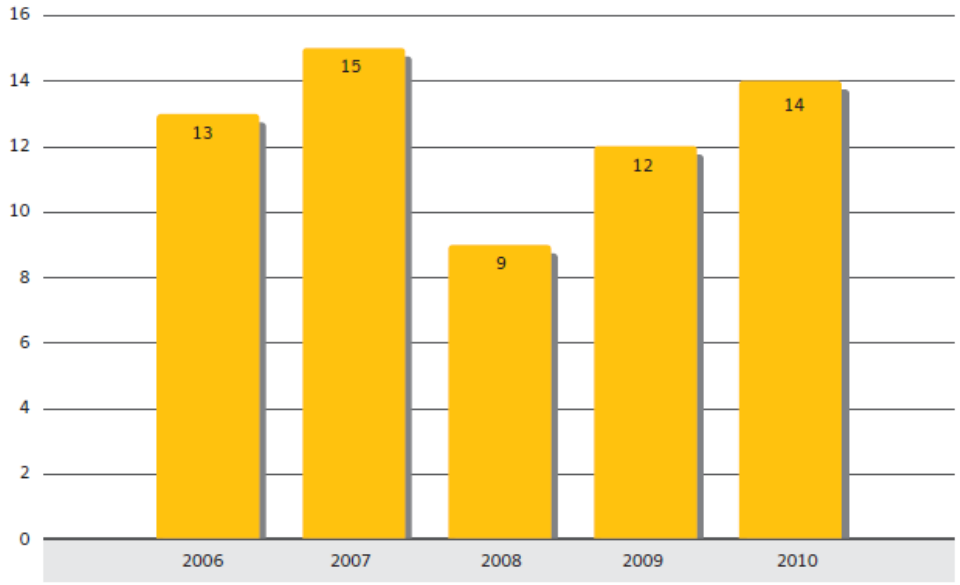
❷ Social networking + social engineering = compromise



❸ Hide and seek (zero-day vulnerabilities and rootkits)

- Although the short term trend in exploits of zero-days vulnerabilities is up, the long term is not

- Nevertheless, zero days are being used in a more aggressive way, e.g. they featured heavily in the targeted attacks of 2010

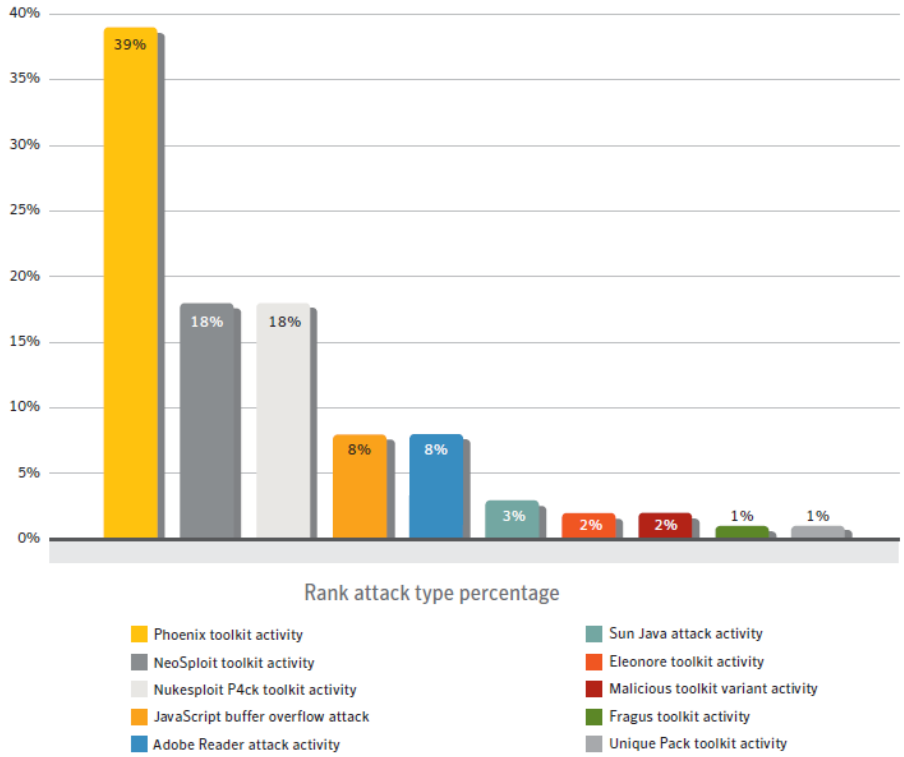


Number of documented 'zero-day' vulnerabilities

- Attack toolkits help to spread knowledge of exploits that leverage vulnerabilities
- Rootkits taking more aggressive hold
  - Tidserv, Mebratix, and Mebroot are current front-runners

❹ Attack kits get a caffeine boost

- Attack kits continue to see widespread use – 61% of web based attacks are due to toolkits.
- Java exploits added to many existing kits
- Kits exclusively exploiting Java vulnerabilities appeared



More Info:

Detailed information available in *ISTR Mid-Term: Attack Toolkits and Malicious Websites*

Threat Activity Trends

Malicious Activity by Country

Source	2010		2009	
	Overall Rank	Overall Percentage	Overall Rank	Overall Percentage
United States	1	19%	1	20%
China	2	16%	2	9%
Germany	3	5%	5	5%
Brazil	4	4%	4	5%
United Kingdom	5	4%	3	6%
India	6	4%	7	3%
South Korea	7	4%	9	3%
Italy	8	3%	10	3%
Taiwan	9	3%	6	4%
Russia	10	2%	8	3%

Threat Activity Trends

Malicious Activity by Country

Bot

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
United States	1	14%	1	13%
Germany	2	10%	5	8%
Taiwan	3	8%	4	8%
Italy	4	7%	6	7%
Brazil	5	7%	3	8%
China	6	6%	2	12%
United Kingdom	7	6%	14	3%
Poland	8	4%	8	6%
Japan	9	3%	11	3%
Spain	10	3%	7	7%

Network Attack Origin

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
United States	1	22%	1	24%
China	2	13%	2	11%
Germany	3	6%	3	10%
United Kingdom	4	6%	4	7%
France	5	3%	5	4%
Brazil	6	3%	6	3%
Italy	7	3%	7	3%
Russia	8	3%	10	2%
Japan	9	3%	9	3%
Spain	10	3%	8	3%

Web-based Attack Origin

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
China	1	67%	3	14%
South Korea	2	13%	5	6%
United States	3	8%	1	24%
United Kingdom	4	4%	2	19%
Australia	5	1%	15	1%
Taiwan	6	1%	4	9%
Russia	7	1%	11	1%
Germany	8	1%	6	2%
Canada	9	< 1%	7	2%
Italy	10	< 1%	9	1%

- The US is the main source of bot-infected computers

  For the botnet associated with the Tidserv Trojan over half of all infected computers are in the US.

- Higher broadband capacity allows more attacks per second

- Large-scale attacks using the ZeuS attack kit contributed to the high-ranking of China for Web-based attacks.

Malicious Activity by Country

Malicious Code

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
United States	1	18%	1	19%
India	2	13%	2	10%
China	3	7%	3	9%
Brazil	4	3%	5	3%
United Kingdom	5	3%	4	4%
Japan	6	3%	8	3%
Turkey	7	3%	11	2%
Saudi Arabia	8	2%	10	2%
Mexico	9	2%	7	3%
Russia	10	2%	12	2%

Spam Zombies

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
Brazil	1	10%	1	16%
United States	2	8%	6	4%
Germany	3	7%	7	4%
India	4	7%	3	6%
Netherlands	5	6%	47	< 1%
Russia	6	5%	2	7%
United Kingdom	7	4%	19	2%
Uruguay	8	4%	35	< 1%
Italy	9	4%	9	4%
Vietnam	10	3%	10	3%

Phishing Hosts

Source	2010 Overall Rank	2010 Overall %	2009 Overall Rank	2009 Overall %
United States	1	46%	1	40%
Germany	2	6%	2	5%
Canada	3	4%	9	3%
United Kingdom	4	3%	6	3%
South Korea	5	3%	4	4%
China	6	3%	7	3%
Netherlands	7	2%	13	2%
Brazil	8	2%	12	2%
France	9	2%	10	2%
Russia	10	2%	5	4%

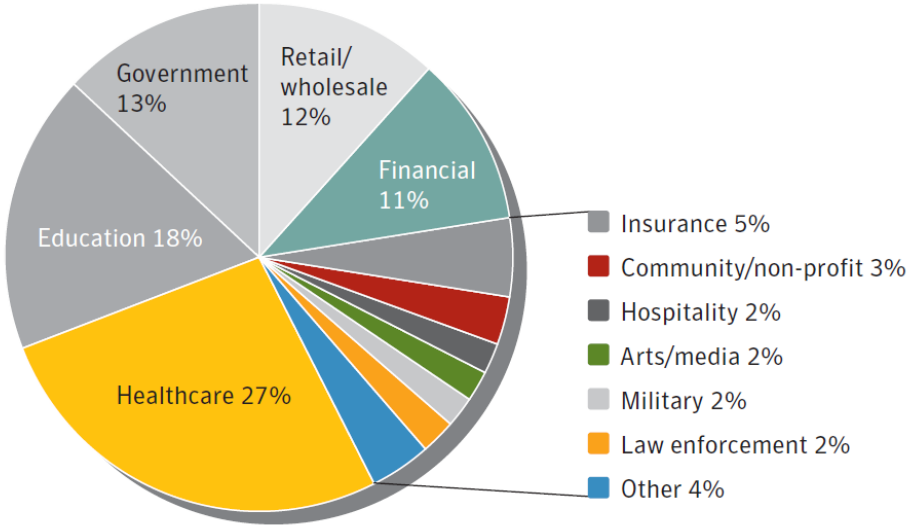
- Spam zombies dropped significantly in China but continue to be a major source of malicious activity in Brazil.

  New regulations requiring ISPs to register email servers and maintain logs in China likely contributed to this drop

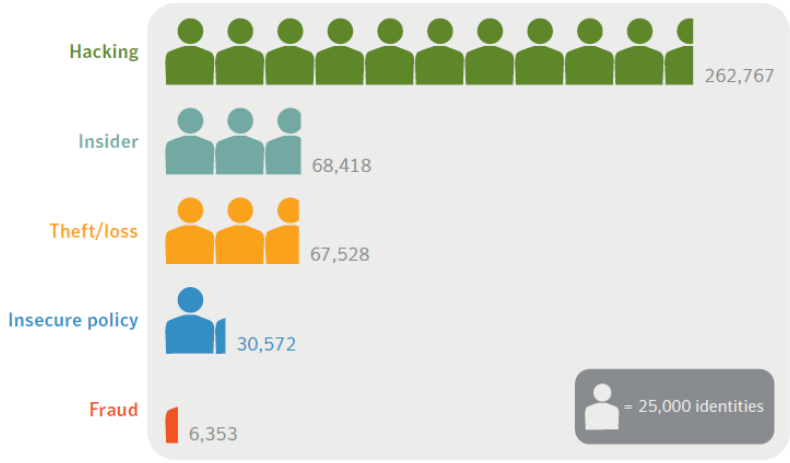
- Phishing host in a country are tied to the broadband connectivity in that country as well as web hosting providers. Many phishing sites are hosted on free web space provided by ISPs.

Data Breaches by Sector

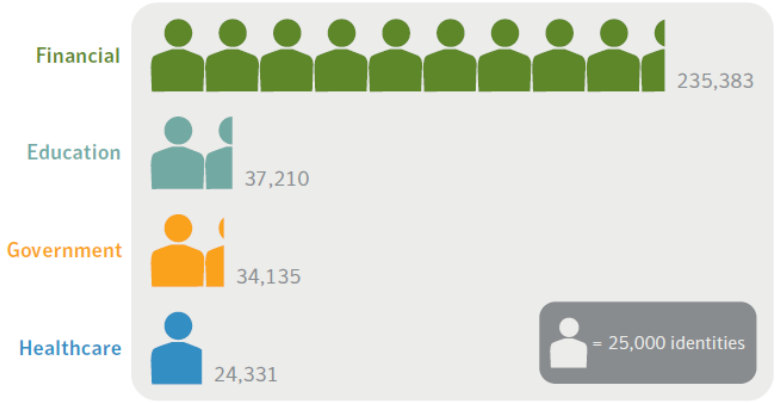
- Top three sectors only accounted for a quarter of all identities exposed
- The average cost to resolve a data breach in 2010 was $7.2 million USD
- Customer data accounted for 85% of identities exposed



Volume of Data Breaches by Sector



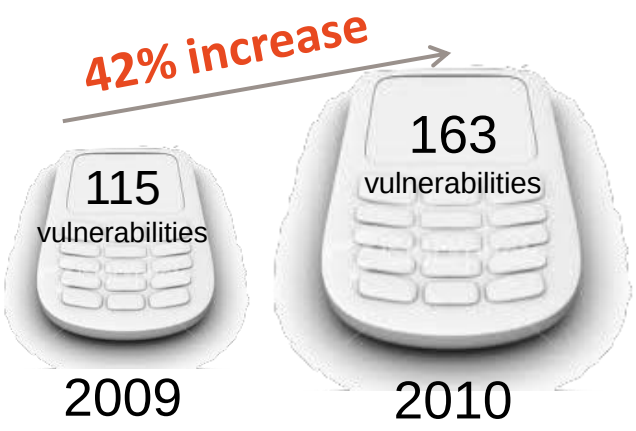
Average Number of Identities Exposed per Data Breach by Cause



Average Number of Identities Exposed per Data Breach by Sector

❺ Mobile threats

- Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications



More Info:

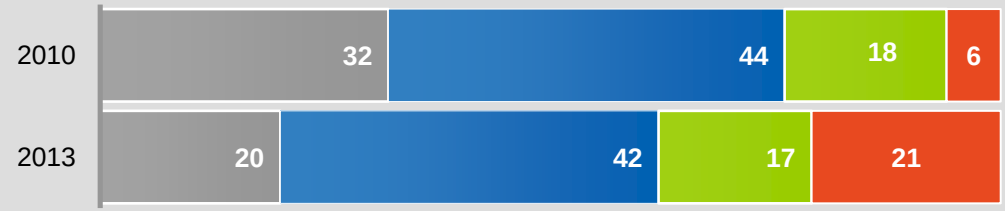
Security Issues for Mobile Devices and a review of Apple iOS and Google Android

- Will be increasingly targeted as they are used for financial transactions

Key Stats In Mobile Growth

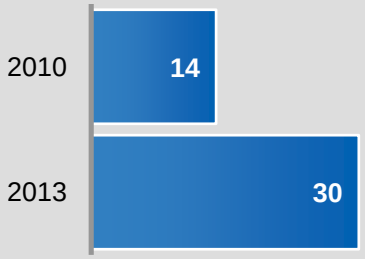
Mobility Enablement Hits an Inflection Point with iPad, iPhone and Android

Tablets Take Hold



Tablets become 21% of mobile devices in 2013*

Smartphone Growth

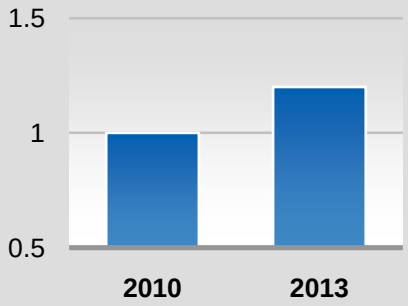


Global smartphone use to double by 2013*

Unmanaged Phones

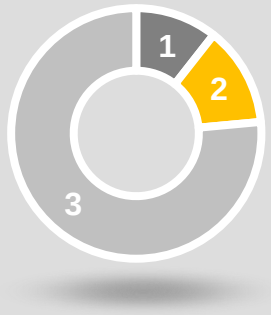
25% of employees use an unmanaged smartphone in 2010*

Mobile Workers



Mobile worker population growing to 1/3rd of the world's workforce in 2013*

Smartphone Access



30% of Information workers to access corp resources via smartphones in 2013**

* Forrester **IDC

Major Shift in Device Usage

Smartphone ownership and internet use summary

% of smartphone owners, cell owners and all adults who…

	% of smartphone owners who…	% of all cell owners who…	% of all adults who…
Own a smartphone	100%	42%	35%
Use the internet or email on smartphone	87	36	30
Use smartphone to go online on a typical day	68	28	23
Go online mostly using smartphone	25	10	8

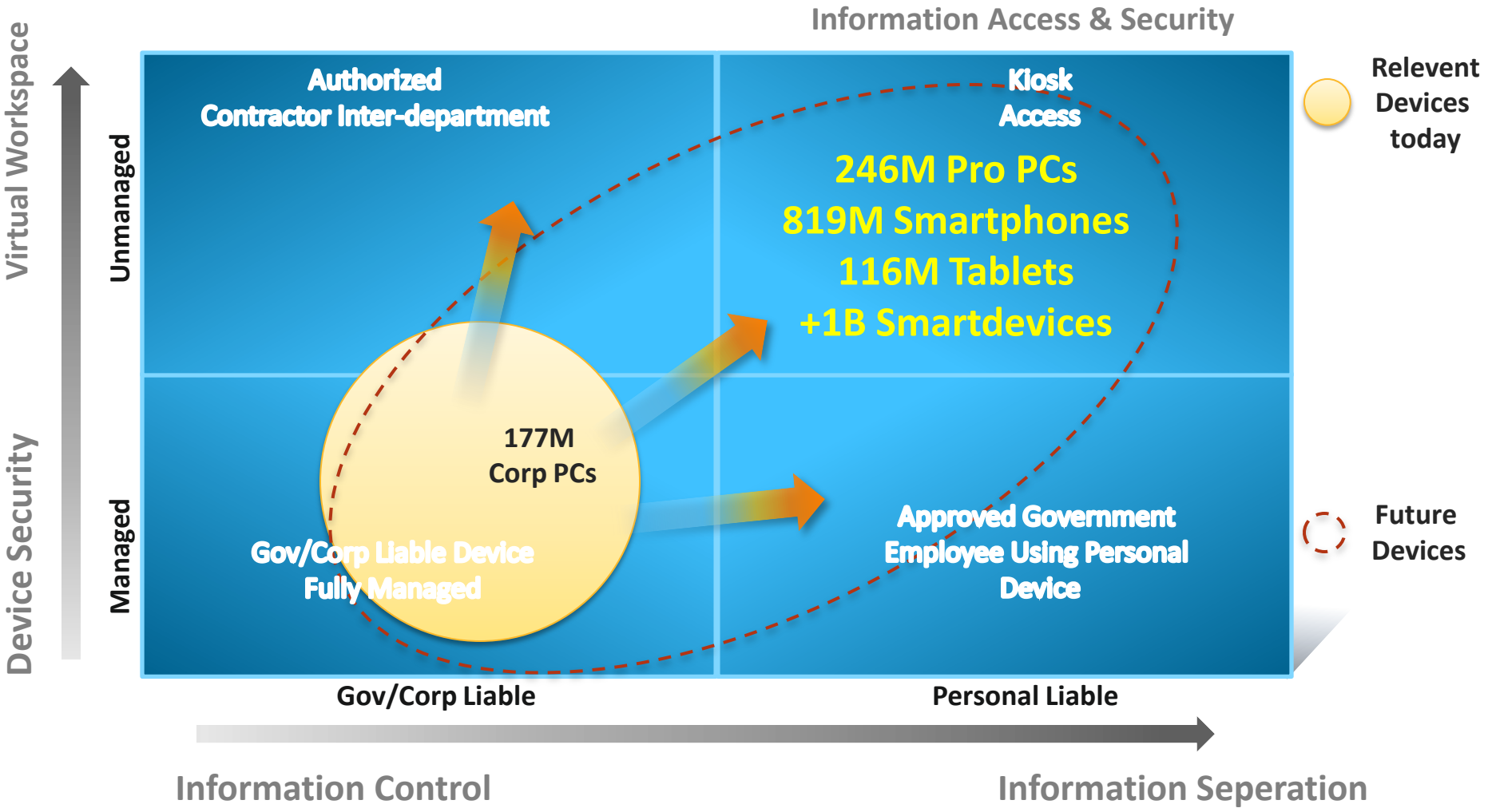
Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey. n=2,277 adult internet users ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish.

Source: Pew Research Internet & American Life Project, July 11, 2011

http://technolog.msnbc.msn.com/_news/2011/07/11/7059067-25-percent-use-smartphones-not-computers-for-majority-of-web-surfing

Consumerization Introduces Unsolved Use Cases

Device explosion shift to include personal & unmanaged



Mobility Creates New IT Challenges

Technology is not enough

Enterprise Mobility Problems

Explosion of New Devices	Increased Risk of Data Loss	New Apps Must Be Supported	Inconsistent Policies
• How do I enterprise-enable these devices?	• How do I protect corporate secrets, protect the brand & comply with regulations?	• How do I manage application deployment & associated costs?	• How do I employ and enforce policy across devices, data usage & application access?

1B+ SmartPhones / Tablets by 2014

Dropbox
Productivity

Facebook
Social Networking

Keynote
Productivity

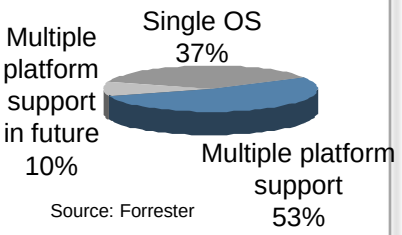
Salesforce Chat...
Business

WorldMate Gol...
Travel

amazon cloud drive

Microsoft Office 365

Mobile platforms in enterprises (2009)



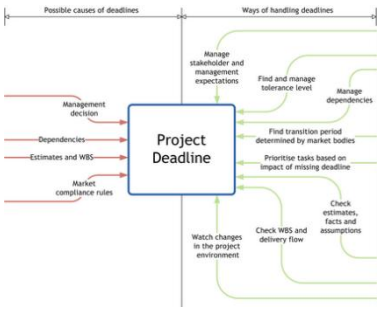
Source: Forrester

Mobility Creates New IT Challenges

Security Processes in Application Development Lagging

Mobile App Security Problems

Extreme Agile Development	Application Data Protection	3rd-Party App Security	App Security Testing
• How do I ensure mobile apps protect data and privacy while meeting customer demands?	• How do you manage application security across varying platforms?	• How do I ensure 3rd-party apps do not introduce security vulnerabilities?	• How do I test mobile apps for security vulnerabilities and privacy concerns?



Symantec Security Defense in Depth:

Visibility
Control
Agility

Global Intelligence

Identity Protection

Information Protection

Infrastructure Protection

Information Protection

Thank you!

www.symantec.com/threatreport
www.symantec.com/stuxnet

Brian J. Tillett

Chief Security Strategist
Symantec Public Sector