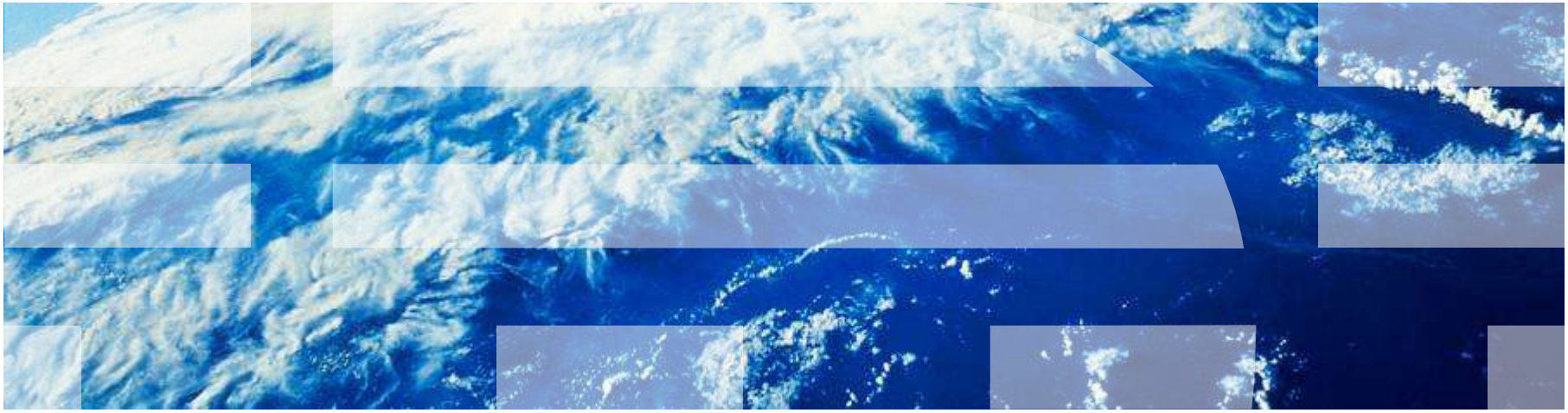
Global Security Trend in 2013 and the importance of IBM Security Philosophy “Secure by Design”



About Me

hjchoi@kr.ibm.com / hyojin.choi@hanmail.net

- **HyungHee University Graduate School**
  - ✓ Major: International Business Management
- **Present: IBM 'Security Systems' Business Unit Executive**
  - ✓Driving the achievement of IBM Security Product (SIEM, SSO, IDM, IPS, Data Masking Tool, Web and Source Scanning Tool) revenue target
  - ✓Developing and promoting IBM Security products solution, current issues, trends and opportunities

The Smarter Planet enables innovative change which inevitably brings new risks…

The planet is getting more …

Instrumented

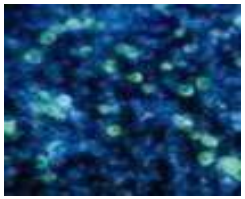
Interconnected

Intelligent


Smart supply chains


Smart countries


Smart retail


Smart water management


Smart weather


Smart energy grids


Intelligent oil field technologies


Smart regions


Smart healthcare


Smart traffic systems


Smart cities


Smart food systems

The world is becoming more digitized and interconnected, consequently opening the door to emerging threats and leaks…

DATA EXPLOSION

The age of Big Data has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more

ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased, coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

A smarter planet creates new opportunities, but also new risks.

The planet is becoming more instrumented, interconnected and intelligent.

New possibilities

New complexities

New risks

"We have seen more change in the last 10 years than in the previous 90."

Ad J. Scheepbouwer, CEO, KPN Telecom

Critical infrastructure protection

Privacy and identity

New and emerging threats

Cloud security

Cybersecurity Landscape

Stakeholders recognize the importance of cyberinfrastructure to our nation's prosperity.

- Public and private sector enterprises today are ***highly dependent*** on information systems to carry out their missions and business functions.
- To achieve mission and business success, enterprise information systems must be ***dependable*** in the face of serious cyber threats.
- To achieve information system dependability, the systems must be appropriately ***protected***.

"…cyber threat is one of the most serious economic and national security challenges we face as a nation."

President Barack Obama

Source: "Information Systems Under Attack", NIST

What is at risk?

Transportation Infrastructure

+

Healthcare Infrastructure

+

Banking & Financial Infrastructure

+

Energy & Utilities Infrastructure

+

Communications Infrastructure

…

A smarter planet introduces several security challenges.

Key drivers for security projects

Managing Compliance

"Non-compliance costs are 2.65 times higher for organizations than compliance costs."[2]

Rising costs of security

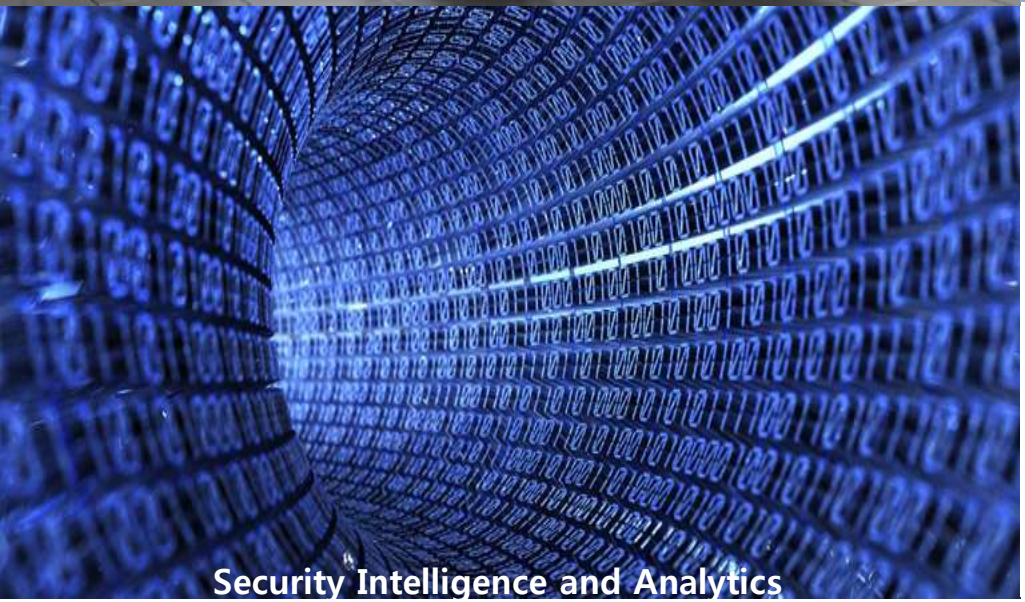
"Average detection and escalation costs went up by 72 percent from 2009 levels"[1]

Rising costs Of breach

"The cost of a data breach increased to **US$214** per compromised customer record and **US$7.2M** per breach event"[1]

[1]Ponemon Institute: Cost of data breaches climbs higher, by Dr. Larry Ponemon, March, 2011 http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher
[2]Ponemon Institute: Compliance like a club, by Dr. Larry Ponemon, January 31, 2011 http://www.ponemon.org/blog/post/compliance-like-a-club

Global Security Trend in 2013

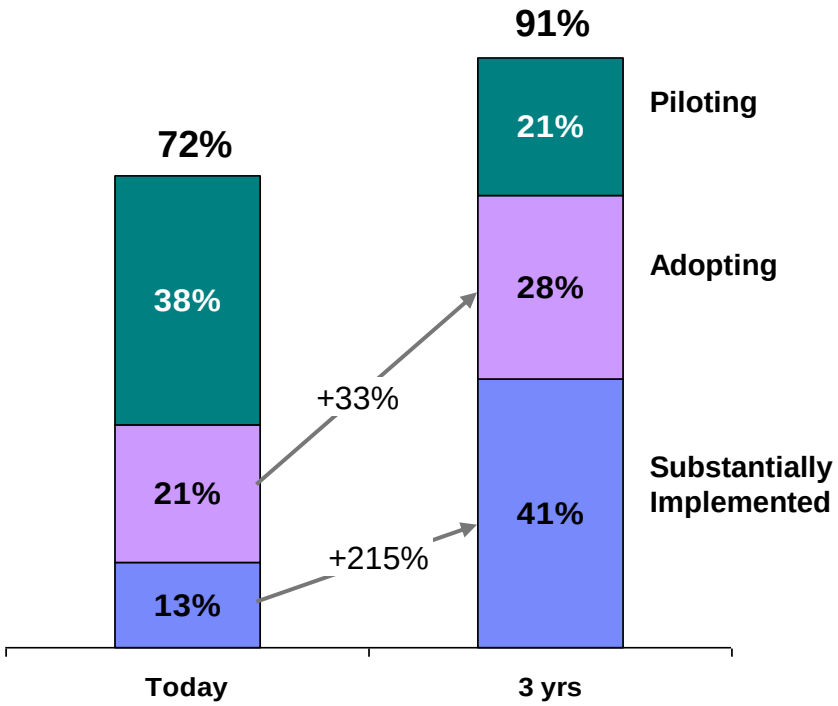



SECURITY PREDICTION #1
In early 2014, cloud security will go from "mystery and hype" to "secure and move-on".
Data, identity and monitoring technologies will continue to emerge to meet requirements of cloud computing, enabling organizations to leverage cloud with the same confidence they do their data center.

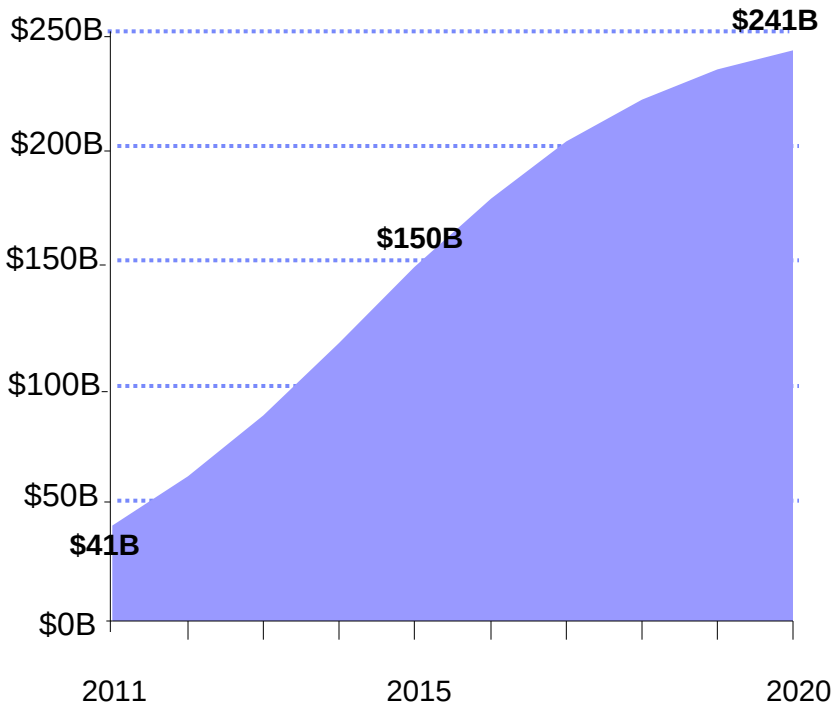
Cloud is widely recognized as an increasingly important technology; adoption is expected to accelerate rapidly in the coming years.

What is Your Organization's Level of Cloud Adoption?

% of Respondents



The Global Cloud Computing Market is Forecast to Grow 22% per year through 2020



Source: Sizing the cloud, Forrester Research, Inc., April 21, 2011

Nearly half (48%) of CIOs surveyed evaluate cloud options first, over traditional IT approaches, before making any new IT investments

Source: (1) 2011 joint IBV/EIU Cloud-enabled Business Model Survey of 572 business & IT leaders; Q4. Which of the following most accurately describes your organisation's level of cloud technology adoption today and which do you expect will best describe it in three years?
Sizing the cloud , Forrester Research, April 21, 2011; http://www.cio.com/article/684338/Survey_CIOs_Are_Putting_the_Cloud_First

Cloud computing changes the way we think about security

In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning IT resources increases - **greatly affecting all aspects of security**

While the security concerns are often shared across the different cloud models the responsibility changes from consumer to provider and this can present unique challenges.

- *High multi-tenancy and data separation*
- *Image management and compliance*
- *Security of the virtual / hypervisor layer*
- *Virtual network visibility*
- *Need for Service level agreements (SLAs)*
- *Provider responsibility for infrastructure*
- *Customization of security controls*
- *Visibility into day-to-day operations*
- *Access to logs and policies*
- *Applications and data are publically exposed*

SECURITY PREDICTION #2

By EOY 2014, mobile devices will be more secure than laptops are today.

Comprehensive mobile security technology now exists to protect almost every part of the mobile experience – from the device, to the network, to the application. On mobile devices, more than on laptops, new attention will be paid to actually securing data in applications.

Mobility, social media, increasing digitization and new analytics capabilities are conspiring to drive broad business change

Major Technology Trends driving Business Change

Mobile revolution

- Connectivity, access and participation are growing rapidly
- Smart devices are becoming the primary route to get connected
- Devices are getting smarter as they are increasingly enriched by mobile apps

Social media explosion

- Social media is quickly becoming the primary communication and collaboration format
- GenY's or "digital natives" use of technology and social media platforms is accelerating adoption
- Enterprises are adopting social media but are struggling to realize the value and manage risk

Hyper digitization

- Digital content is produced and accessed more quickly than ever before
- Internet traffic is growing globally driven by consumer use of video, mobile data, interconnectedness
- An increasing number of connected devices and sensors is further driving growth

The power of analytics

- New capabilities for real time analysis, predictive analytics and micro-segmentation are emerging
- Top performing companies use analytics to drive action and business value
- Analytics are making information "consumable" and is transforming all parts of the organization, from customer intimacy to supply chain management

Source: IBV Analysis

Demand for mobile continues to skyrocket

By 2016, over

350 million

people will use their smartphones for work.[1]

44%

of respondents use their devices for both personal and business purposes. Fewer than

4%

use them strictly for business.[2]

- By 2013, **80 percent** of businesses will support a workforce **using tablets**[3]
- By 2014, **90 percent** of organizations will support corporate applications on **personal devices**[3]

[1]*Forrester Research, Mobile is the New Face of Engagement, February 2012*
[2]*Kathleen Bela and Danielle Hamel, Risky Business: Survey Shows Smartphone Security Concerns Running High, http://www.juniper.net/us/en/company/press-center/press-releases/2010/pr_2010_10_26-10_02.html (2010)*
[3]*Daryl Plummer, Gartner's Top Predictions for 2011: IT's Growing Transparency and Consumerization*

The consumerization of mobile IT is driving change in the workplace

476 million

Vendors shipped a total of 476 million smartphones in 2011 – growing at 27% through 2015

62 percent

Smartphone usage for business by individual–liable (BYOD*) devices in 2014, compared to 38 percent corporate-liable[2]

26 times

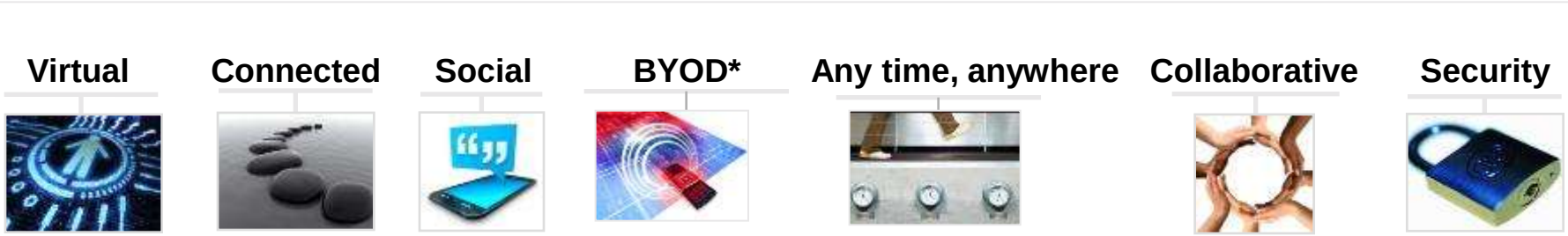
Mobile data traffic is expected to grow 26–fold between 2010 and 2015[3]

1.3 million

By the end of 2011, there will be over 1.3 million applications on smartphones and tablets versus 75 thousand on PCs[4]

10 billion

Number of mobile-connected devices by 2020[5]



*Bring-your-own-device

1. IDC, "Worldwide Quarterly Mobile Phone Tracker," June 2011; 2. IDC, "Worldwide Business Use Smartphone Forecast and Analysis," doc #225054, September 2010; 3. Gartner, "Forecast: Mobile Data Traffic and Revenue, Worldwide, 2010-2015," July 2011 ID:G00213763; 4. IDC Insight, Nicholas McQuire, IDC #LM51T Vol. 1, May 2011; 5. The Economist, "Beyond the PC," October 2011

All of these workplace shifts are forcing IT to confront new issues in their mobile infrastructures and in the way they deliver services

"I need to manage the **proliferation of devices** and help employees use their smartphones and tablets in the business?"

"What is the best way to **protect data** and help **ensure compliance** for my desktop and mobile users?"

"I need a cost-effective way to **foster collaboration** and improve productivity … "

"How do I deal with the **complexity** of devices, manage applications and network connections in my enterprise?"

"How can my **service desk** keep up with the changing needs and requirements of my end users?"

Bring Your Own Device (BYOD) challenges are top of mind with CIOs

Bring Your Own Device (**BYOD)** refers to the use of personally chosen smartphones, tablets and PCs for business purposes.

44%

of respondents use their devices for both personal and business purposes. Fewer than

4%

use them strictly for business.

A 2010 study found

81%

of users admit using their devices to access their employer's network without their employer's knowledge or permission.

58%

do so every day.

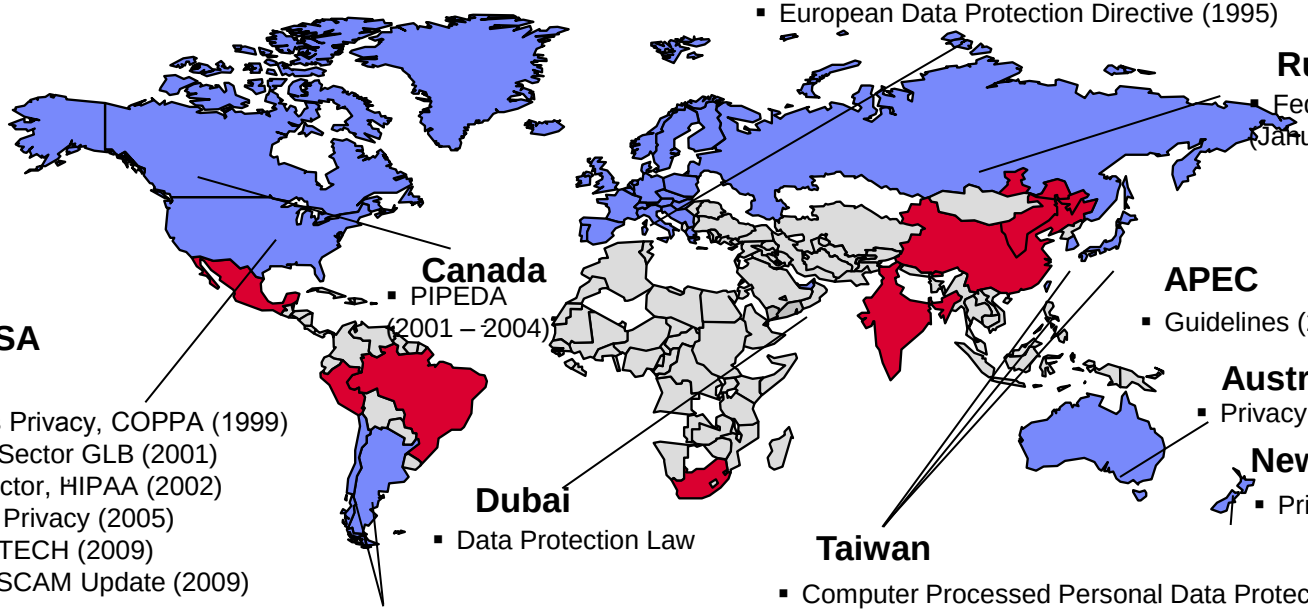
Healthcare: Clinicians want to use their own ipads or smartphones to access patient data whenever and wherever needed while ensuring patient data privacy.

Banking: Loan officers need secure access to corporate email, contacts, and calendar from personally-owned smartphones and tablets.

Education: Universities need to monitor and adjust pre-paid carriers data plans for smartphones as students enter and leave campus wireless network.


SECURITY PREDICTION #3
Compliance will remain a surprisingly robust security driver through 2015, driven by country-level cyber efforts maturing.
New and evolving breaches have set new regulations in motion, presenting new challenges and requiring solutions to adapt and help ensure private information stays private.

Compliance – Data and Privacy



European Union
- European Data Protection Directive (1995)

Russia
- Federal law on Personal Data (January 2007)

Canada
- PIPEDA (2001 – 2004)

APEC
- Guidelines (2004)

USA
- Children's Privacy, COPPA (1999)
- Financial Sector GLB (2001)
- Health Sector, HIPAA (2002)
- California Privacy (2005)
- HIPAA/HITECH (2009)
- FISMA/FISCAM Update (2009)

Australia
- Privacy Amendment Act (2001)

New Zealand
- Privacy Act (1993)

Dubai
- Data Protection Law

Taiwan
- Computer Processed Personal Data Protection Law (1995)

Existing Private Sector Privacy Laws

Emerging Private Sector Privacy Laws

Chile
- Protection of Private Life Law (1999)

South Korea
- Privacy Act (2011)

Argentina
- Protection of Personal Data Law (2000)

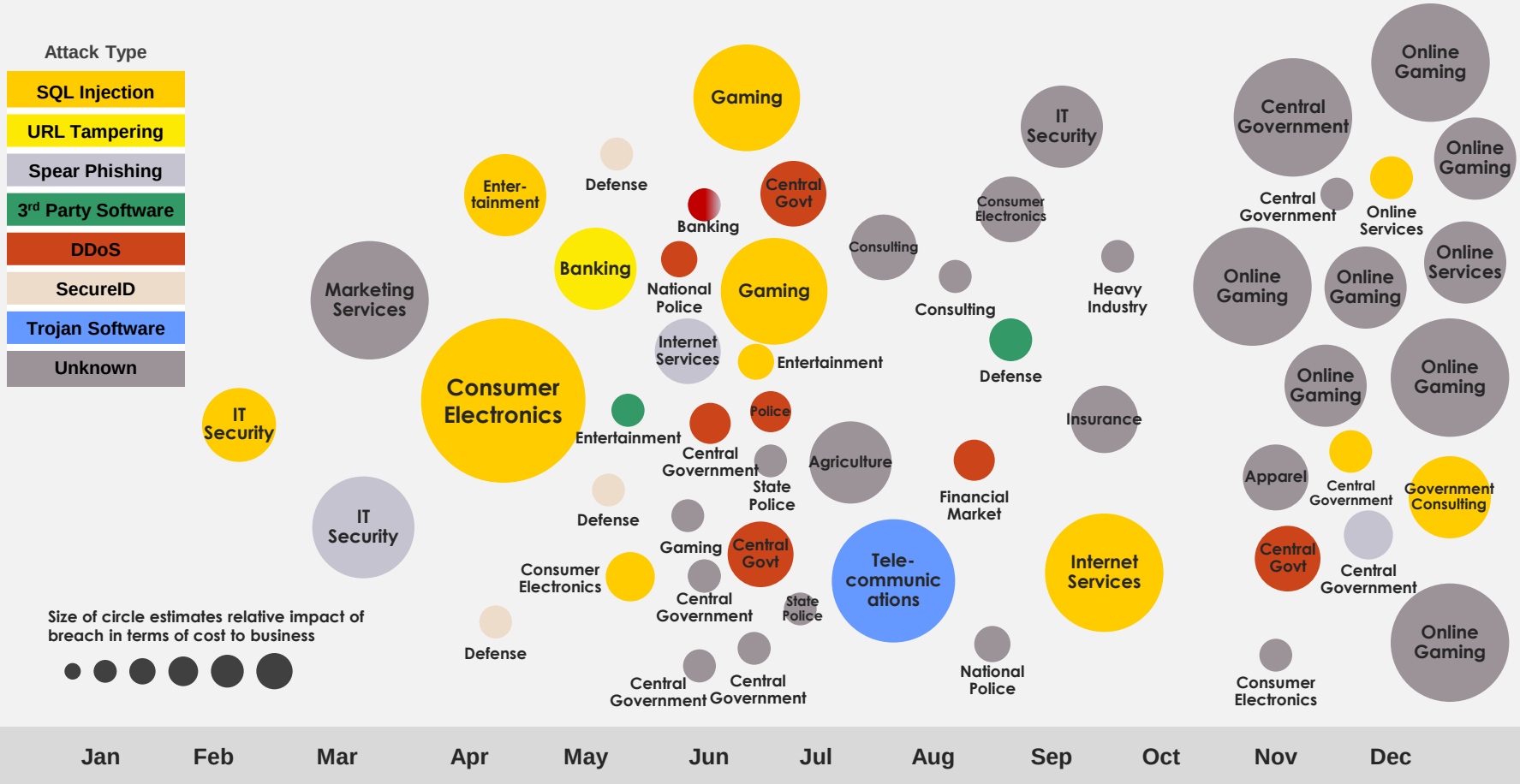
Japan
- Personal Data Protection Act (2005)

SECURITY PREDICTION #4

The type of data collected and inspected to detect advanced threats will balloon in *variety* and *volume* by 2016.

As the security perimeter evolves, so will the attacks – requiring wider analysis of more and more unorthodox data. Advanced organizations are moving beyond security data to find the needle in the haystack.

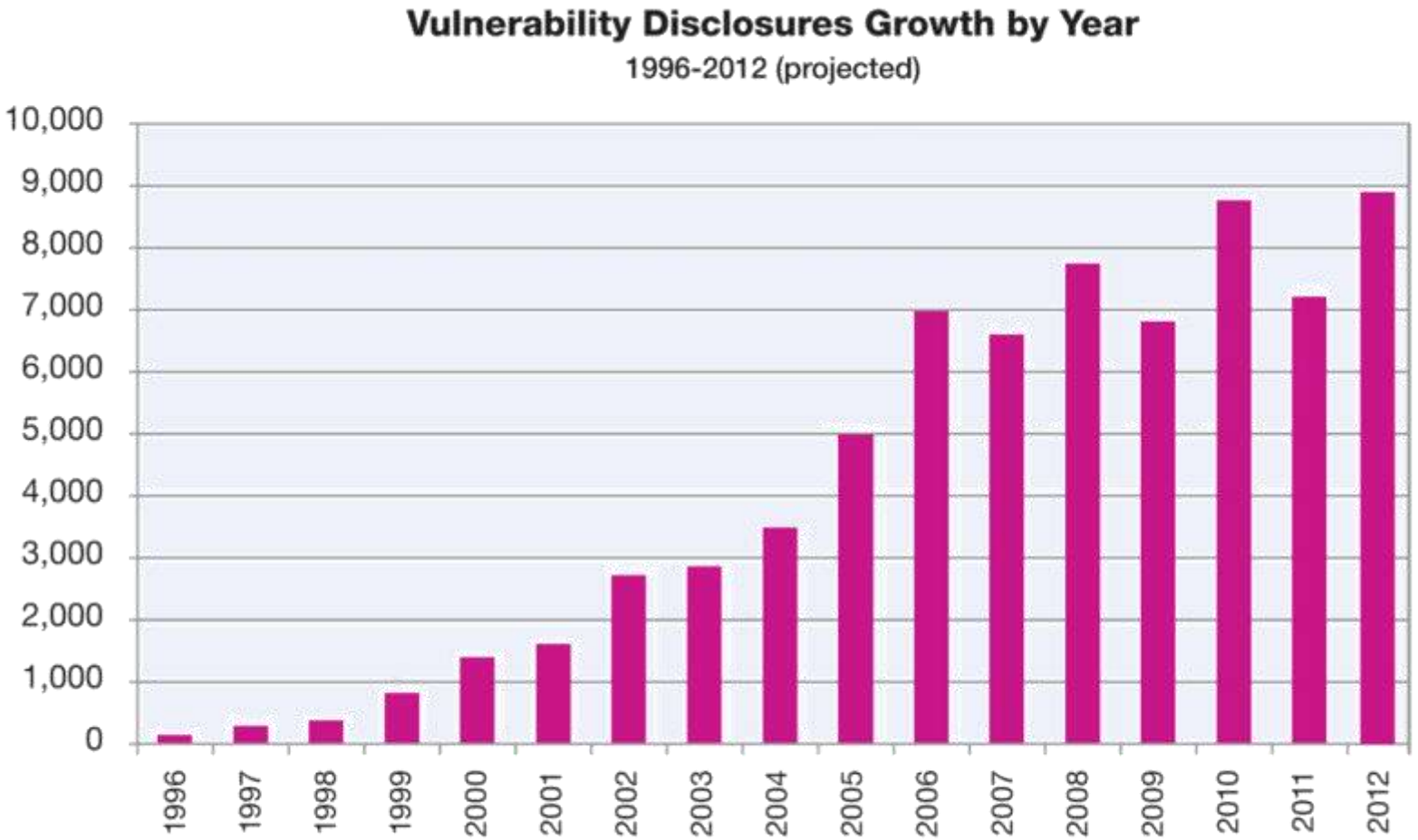
2011: “The year of the targeted attack”



Source: IBM X-Force® Research 2011 Trend and Risk Report

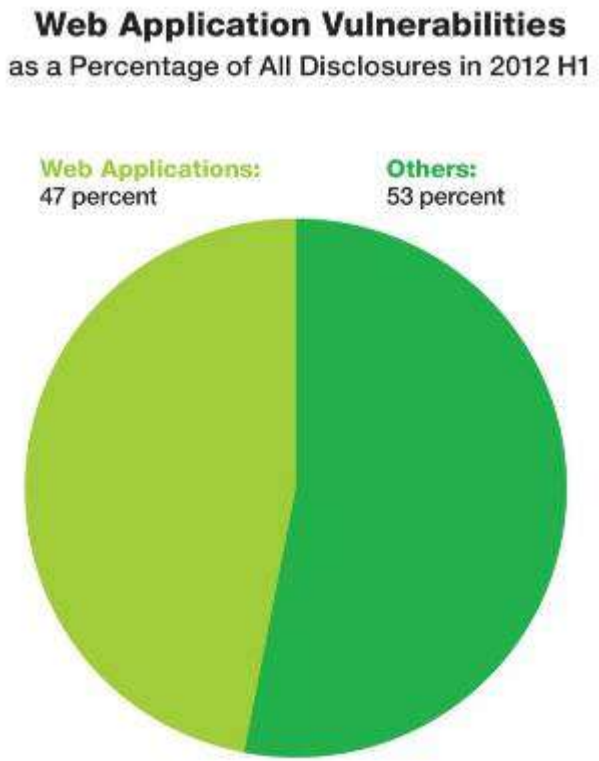
Vulnerability disclosures up in 2012

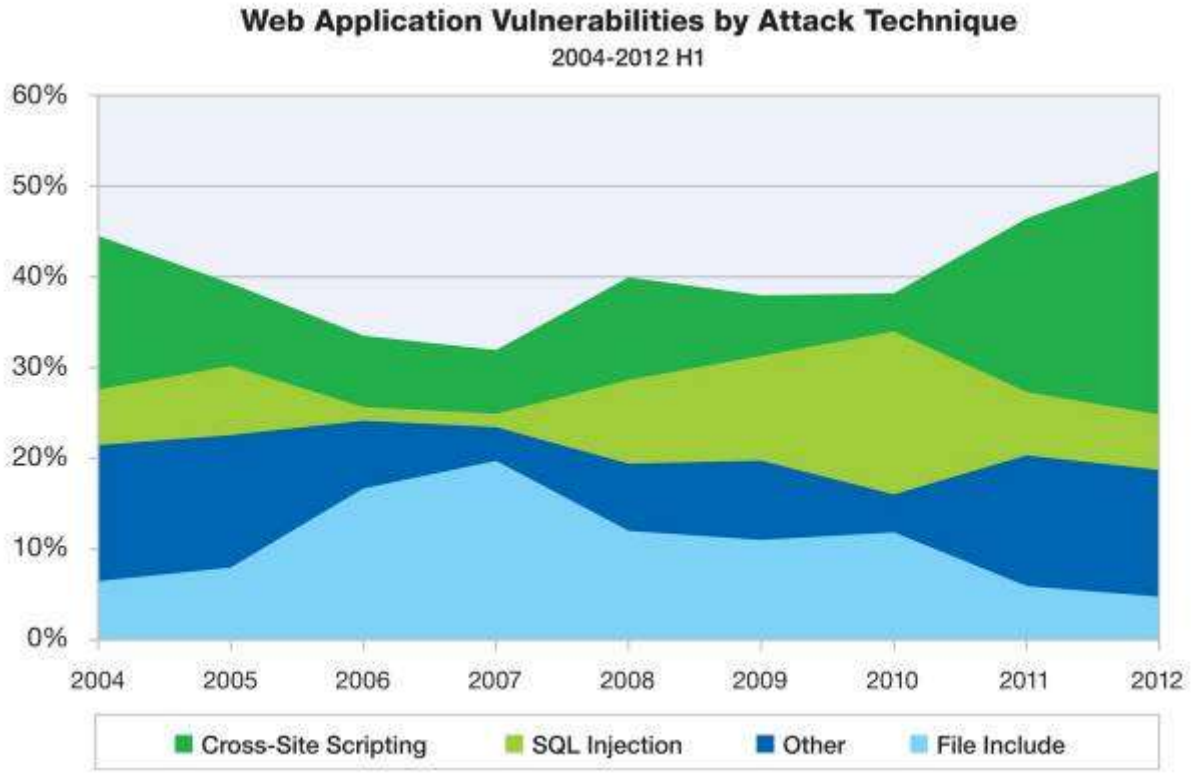
- Total number of vulnerabilities grew (4,400 in 1H 2012)
  - the projection could reach all time high in 2012



Web Application Vulnerabilities Rise Again

- At mid-year 2012, 47% of security vulnerabilities affected web applications
  - Up from 41% in 2011
  - XSS reaches high of 51%





A Big Data Approach to Security Intelligence

Data is everywhere, and savvy organizations are discovering the value of using big data technologies to collect, monitor, analyze and gain insight from security and enterprise data in a manner not previously possible.

Organizations are now able to sift through massive amounts of data — both inside and outside the enterprise — to uncover hidden relationships, detect attack patterns and stamp out security threats.

They're asking questions they could never ask before by examining new sources of data for evidence of a security breach, including a variety of unstructured data sources like customer transactions, email and network and flow data.

They're using sophisticated analytics to discover and investigate high-risk behavior across a variety of enterprise communications channels, so that they're prepared and ready before an incident takes place.

Thanks to analytics, organizations in different industries are discovering the value of being able to look at years worth of data to spot anomalies and subtle indicators of attack.

Using these new tools, a financial services company can uncover fraud by correlating real-time and historical account activity to spot abnormal user behavior, unlikely application paths and suspicious transactions.

A global telecom provider can collect and monitor data on one million events per second — more than 85 billion events per day — to make sure its operations are secure and meet compliance requirements.

To learn more, please visit: ibm.com/security

IBM Curiosity Shop

IBM Security Philosophy

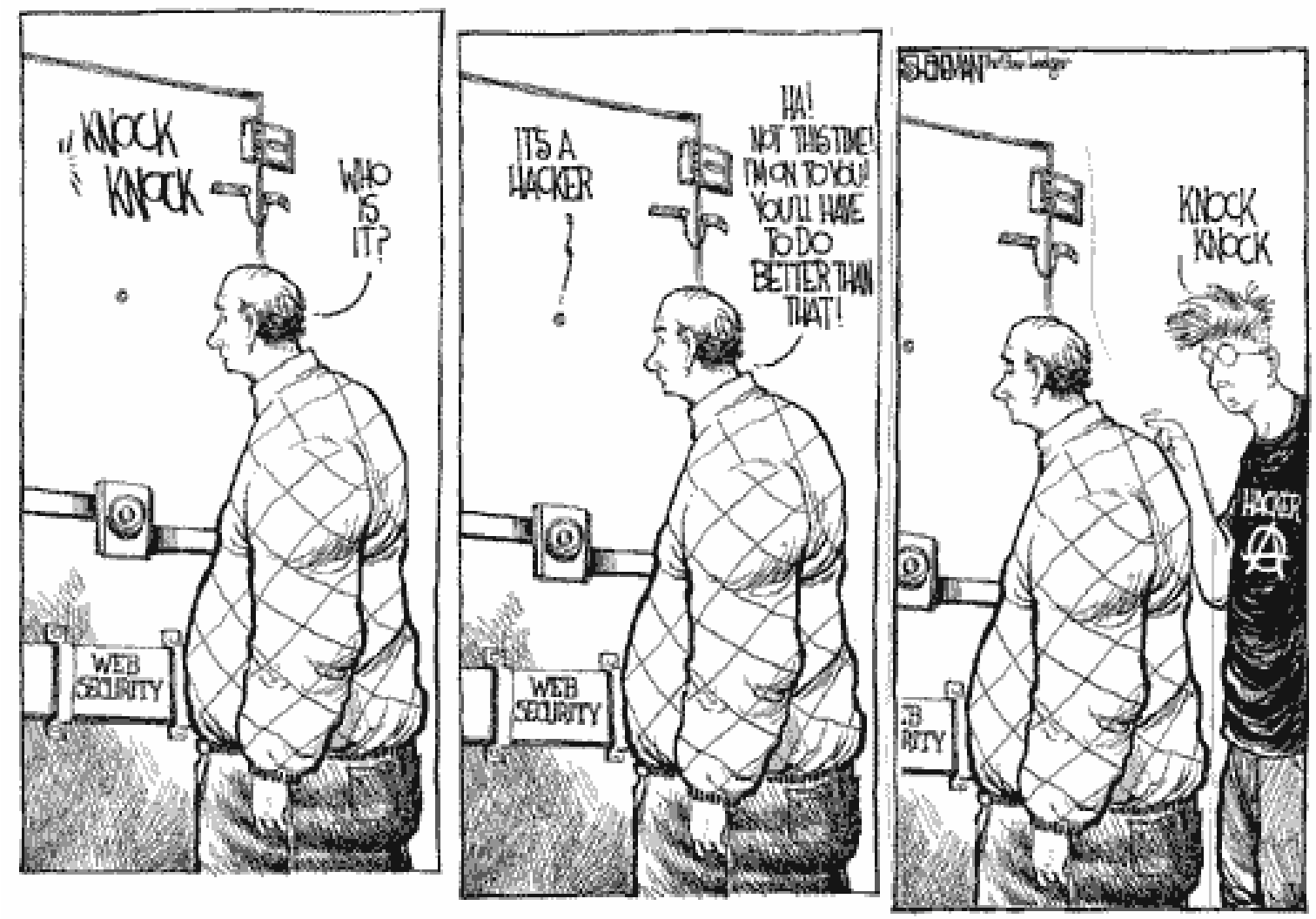
Secure by Design

Workload Driven

Service Enabled

Innovation Powered

Why it is important, Secure by Design?

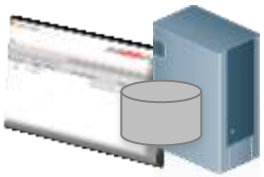


What is SDLC?

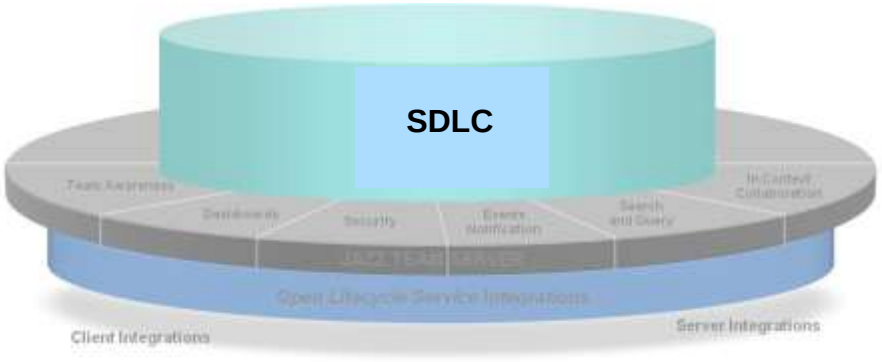
- SDLC? Secure Development Life Cycle.

Applications: Ensuring applications are Secure-by-Design

Application Security Testing is integrated with collaborative lifecycle management tools, ensuring security is effectively addressed during the Software Development Lifecycle



Application Vulnerability Testing



Secure Coding is Compliance!

제목	정보시스템 구축시 SW 개발보안 적용 의무화	게시일	2012-03-27
게시자	홍보담당관실	조회수	1688

"전자정부 시큐어코딩으로 사이버위협에 선제대응"
- 행안부, 정보시스템 구축시 SW 개발보안 적용 의무화 -

앞으로 해킹·분산서비스거부(DDoS) 공격 등에 대한 전자정부서비스의 보안체계가 획기적으로 개선된다.

행정안전부는 사이버공격의 주요 원인인 소프트웨어 보안약점을 전자정부서비스 개발단계에서 제거하기 위해 금년부터 개발되는 정보시스템에 「소프트웨어 개발보안(시큐어코딩)」을 의무화하기로 했다고 밝혔다.

Government decided to make 'Secure Coding' a compulsory for public projects with 4M USD value.

That trend will be cascaded to every industry in Korea.

또한, 행정안전부는 '소프트웨어 개발보안' 제도의 조기 정착을 위해 다음과 같이 기반 조성을 추진할 계획이다.

Cost is a significant driver

80% of development costs are spent identifying and correcting defects!*

During the
CODING phase
$80/defect

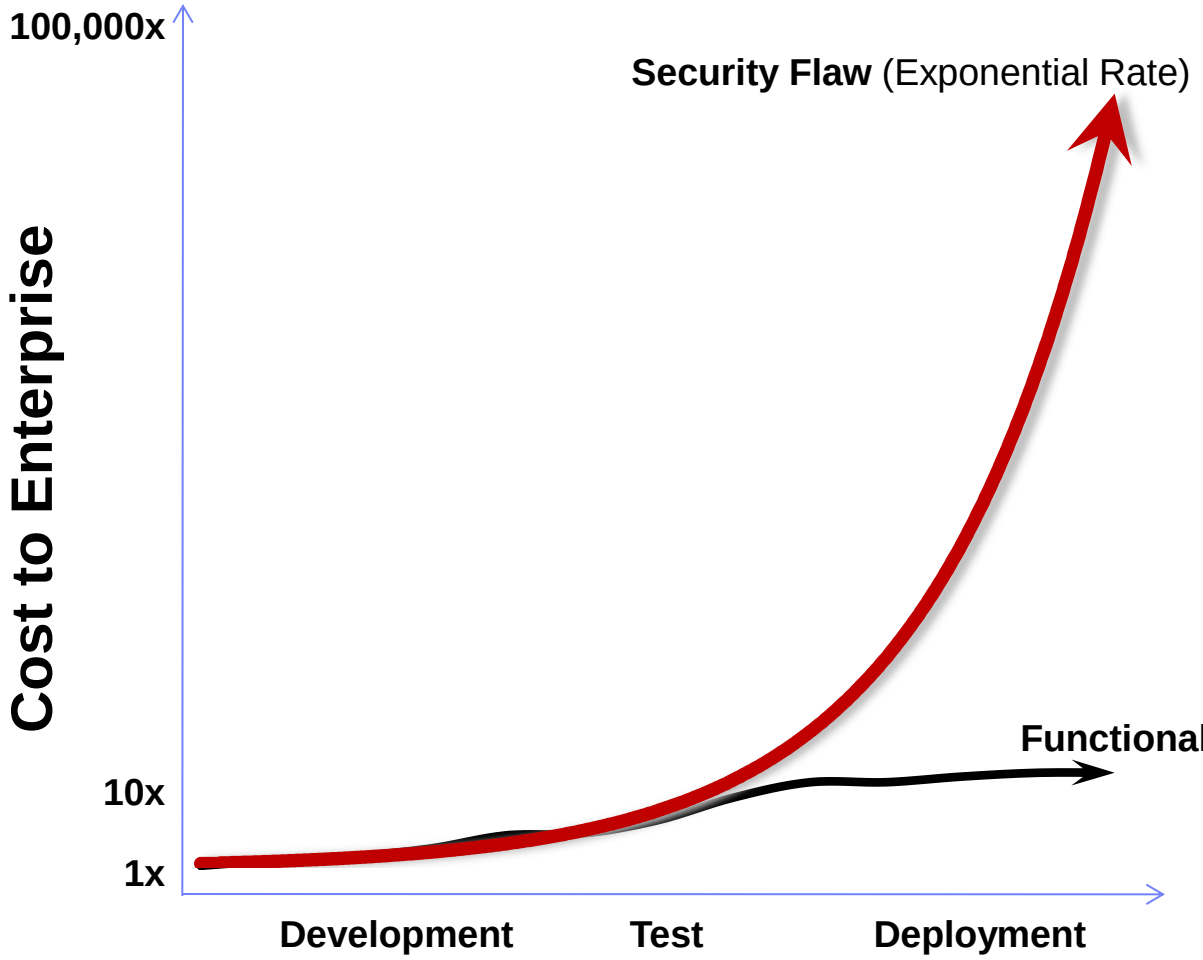
During the
BUILD phase
$240/defect

During the
QA/TESTING
phase
$960/defect

Once **released**
as a product
$7,600/defect
+
Law suits, loss of customer trust, damage to brand

*National Institute of Standards & Technology
Source: GBS Industry standard study
Defect cost derived in assuming it takes 8 hrs to find, fix and repair a defect when found in code and unit test.
Defect FFR cost for other phases calculated by using the multiplier on a blended rate of $80/hr.

Sources of incremental security breach costs



Unbudgeted Costs:

- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair

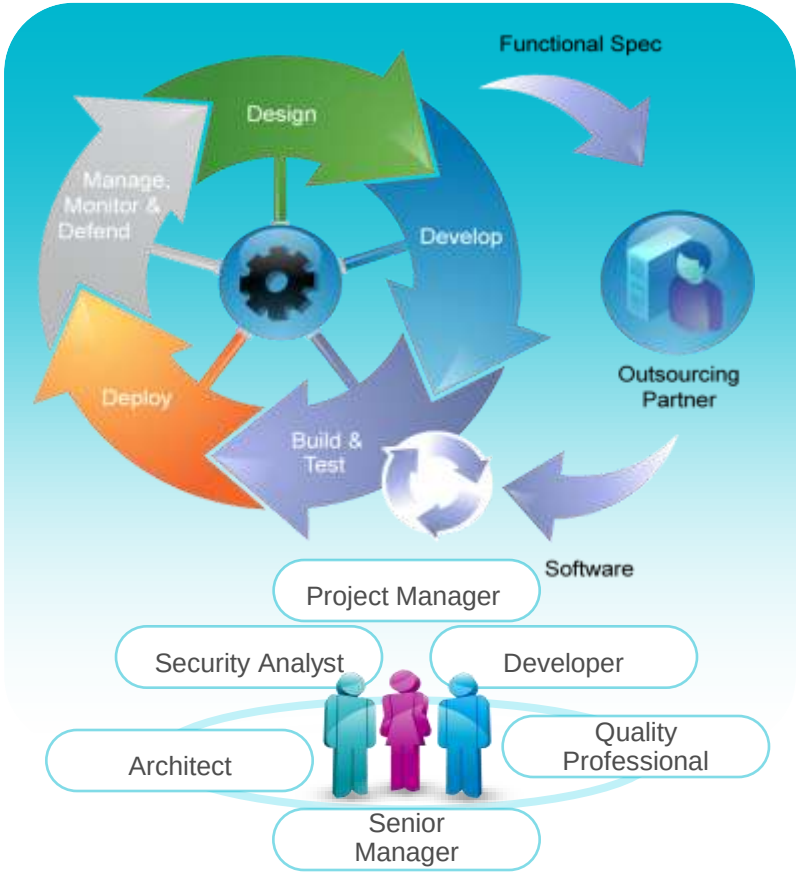
Cost per Record: $214*

Cost per Breach: $7.2M*

* Source: Ponemon Institute 2011

Need to take a proactive approach to Security

- **Embed and integrate security testing early** in the development lifecycle to support agile delivery demands
- Adopt a **Secure by Design** approach to enable the design, delivery and management of smarter software and services
- Bridge the gap between “Security” and “Development” through **joint collaboration and visibility**, enabling regulatory compliance



Baseline of Defense: where we start the security testing..