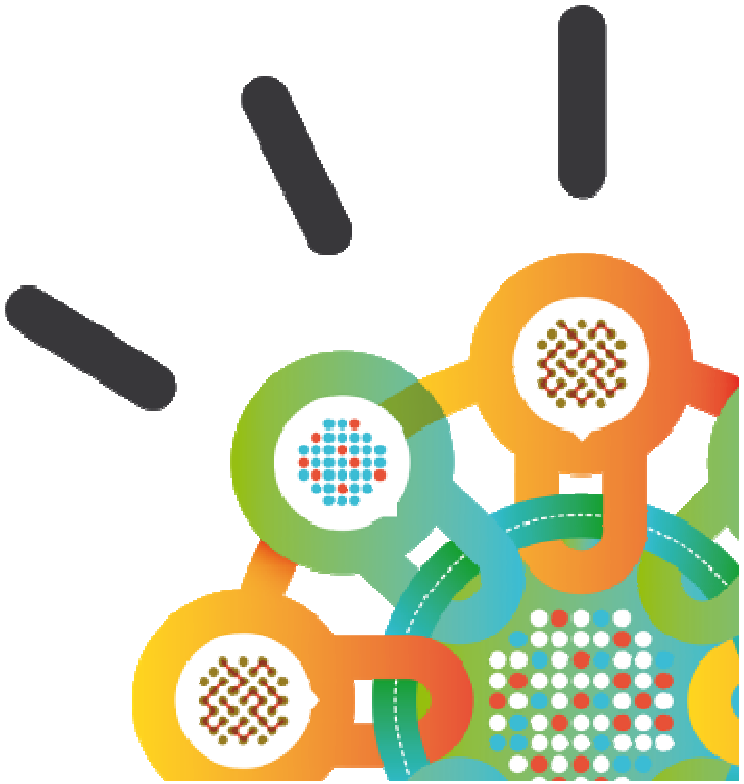
Security Intelligence.
Think Integrated.

IT Security: Current Landscape and 2012 Predictions

Paul Kaspian
Senior Product Marketing Manager
IBM Security Systems



X-Force research

One of the most renowned commercial security research & development groups in the world

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities

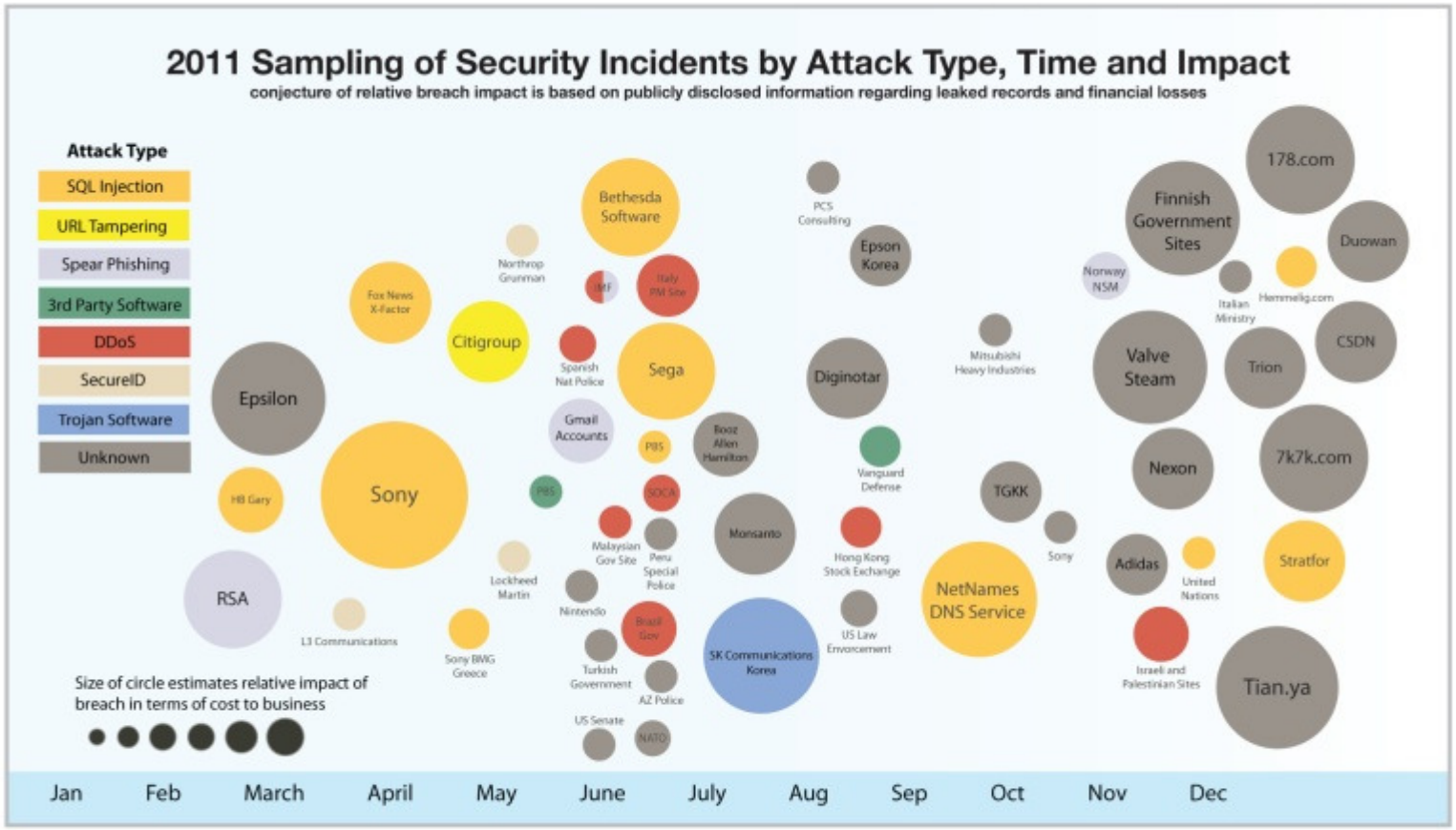
X-Force Research

14B analyzed Web pages & images
40M spam & phishing attacks
54K documented vulnerabilities
13B security events daily

Provides Specific Analysis of:

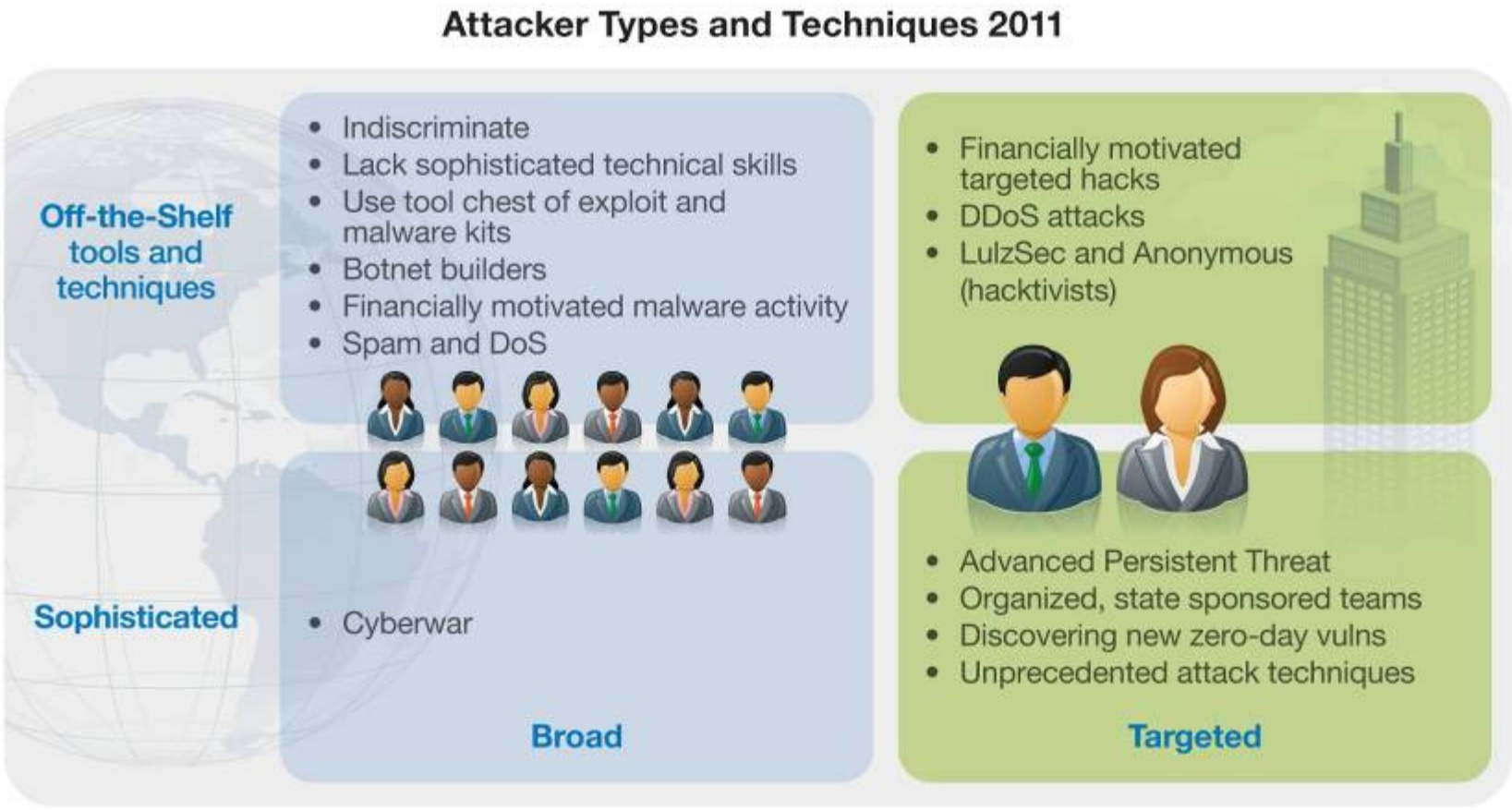
- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

2011: Year of the security breach



Source: IBM X-Force® Research and Development

Who is attacking our networks?

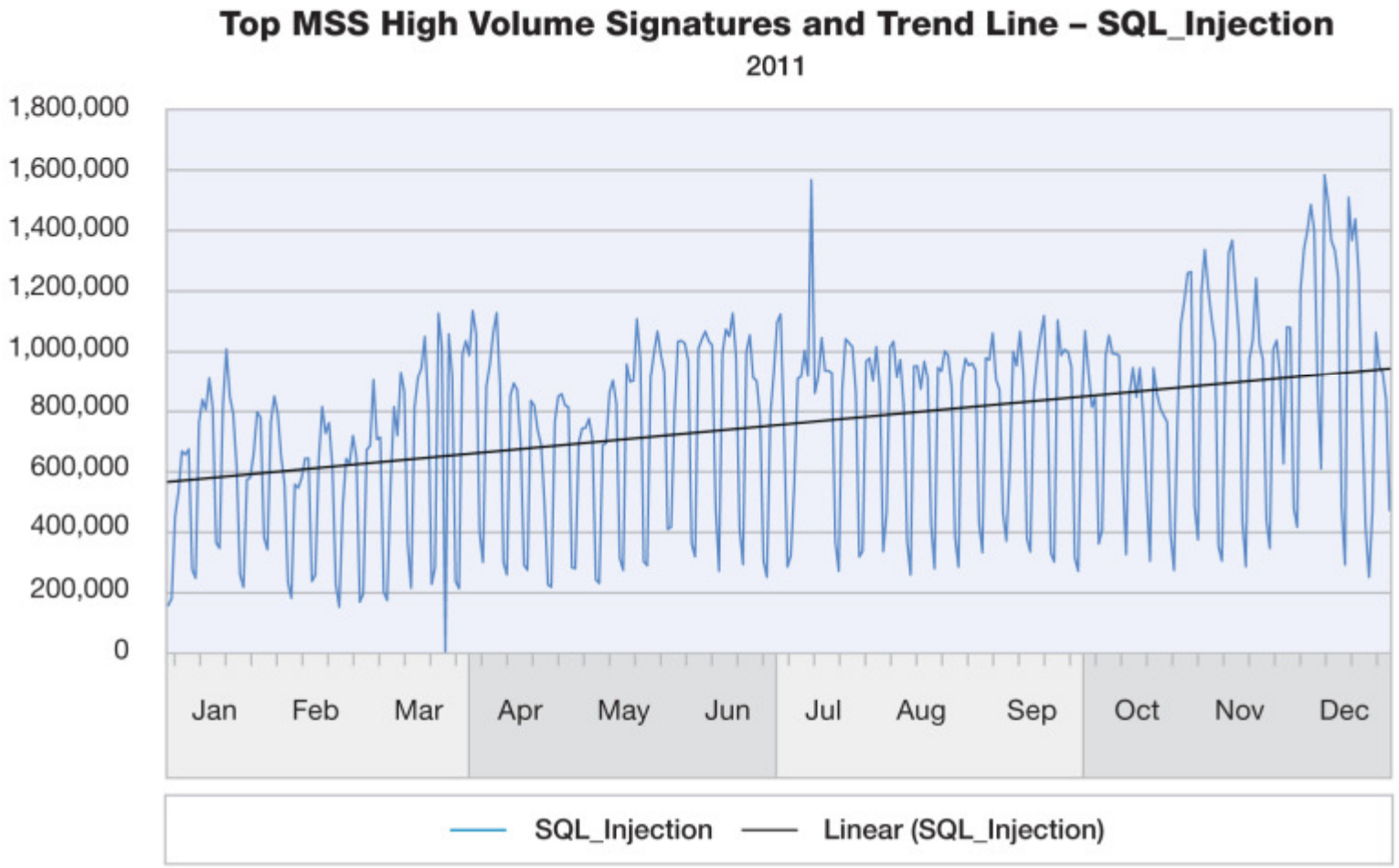


Source: IBM X-Force® Research and Development

Key Messages from the 2011 Trend Report

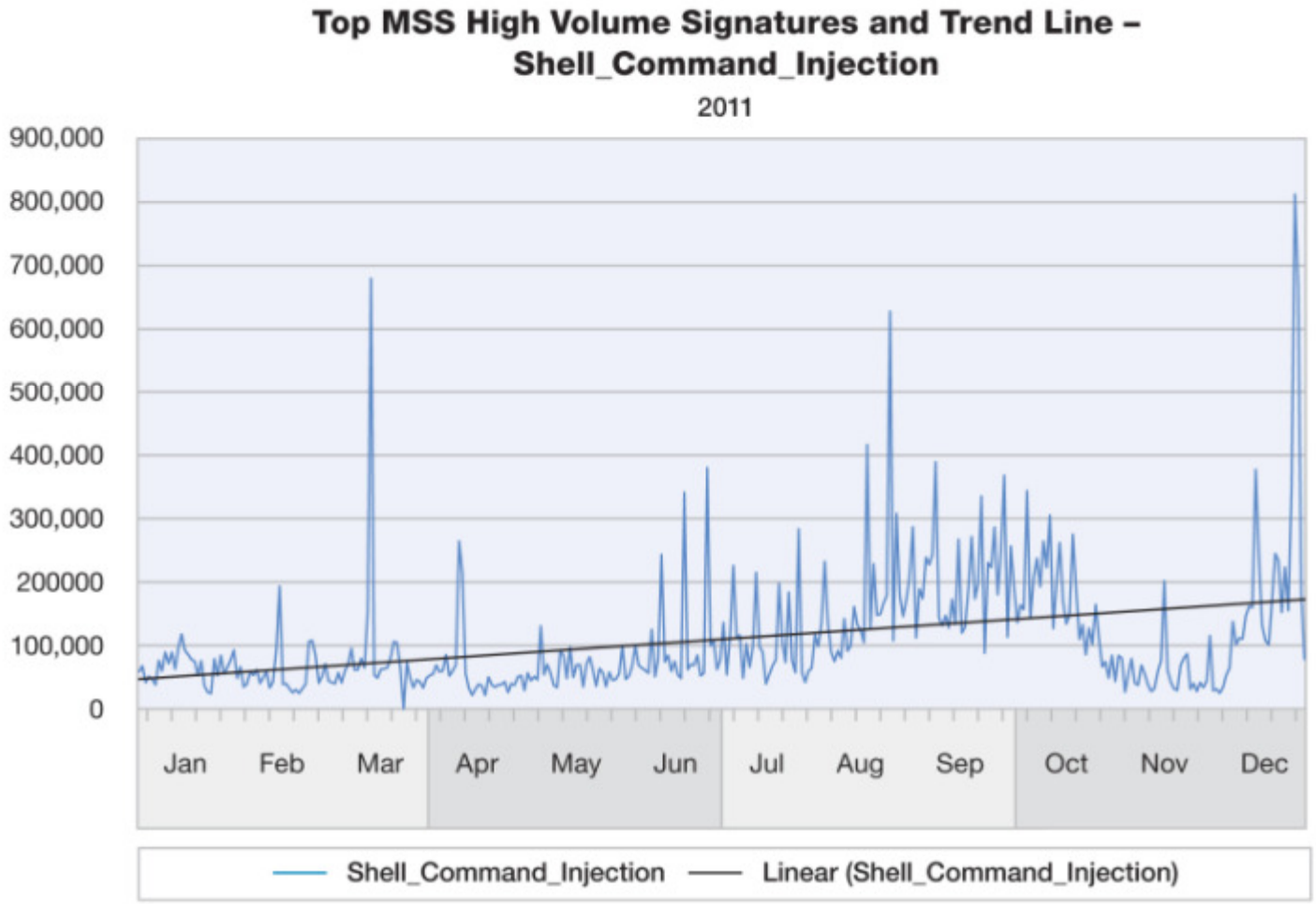
- New Attack Activity
  - –Rise in Shell Command Injection attacks
  - – Spikes in SSH Brute Forcing
  - – Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - – Fewer exploit releases
  - – Fewer web application vulnerabilities
  - – Better patching
- The Challenge of Mobile and the Cloud
  - – Mobile exploit disclosures up
  - – Cloud requires new thinking
  - – Social Networking no longer fringe pastime

SQL injection attacks against web servers



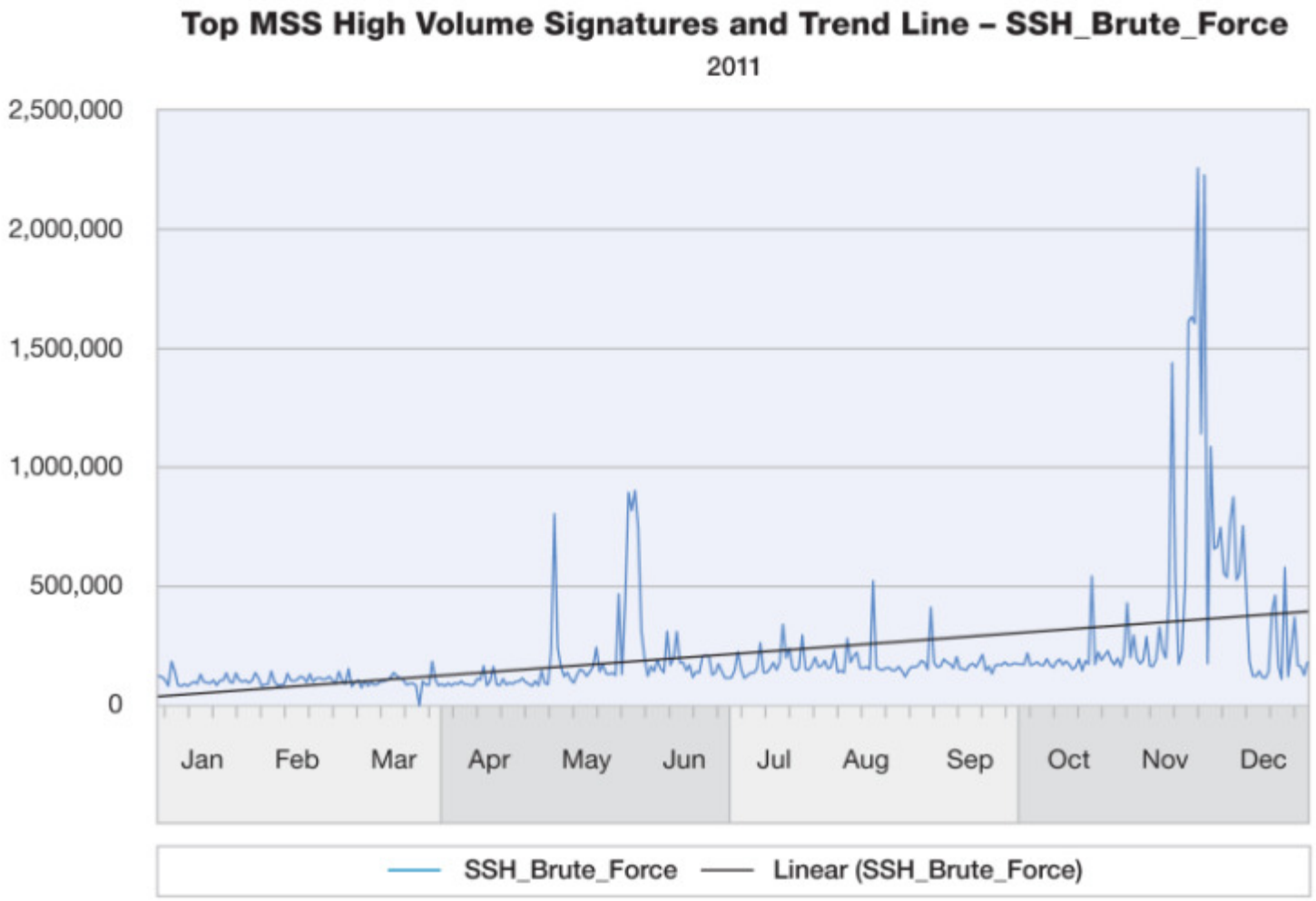
Source: IBM X-Force® Research and Development

Shell Command Injection attacks



Source: IBM X-Force® Research and Development

SSH brute force activity



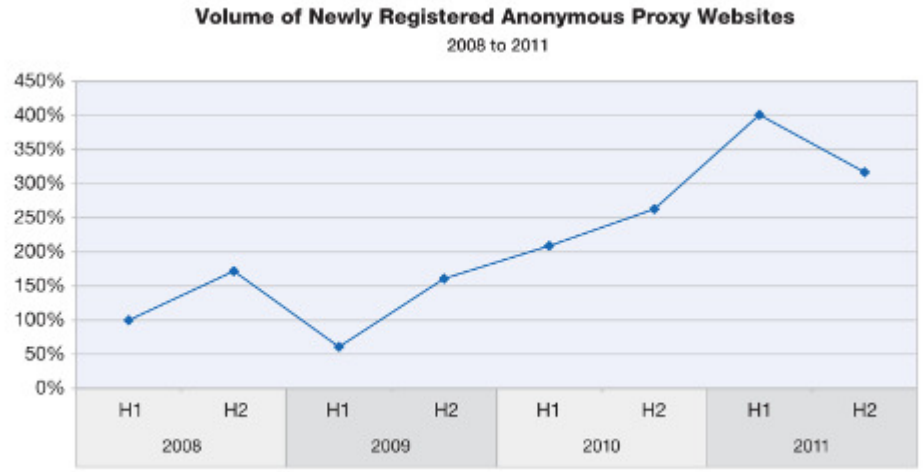
Source: IBM X-Force® Research and Development

Explosion of phishing based malware distribution and click fraud

Source: IBM X-Force® Research and Development

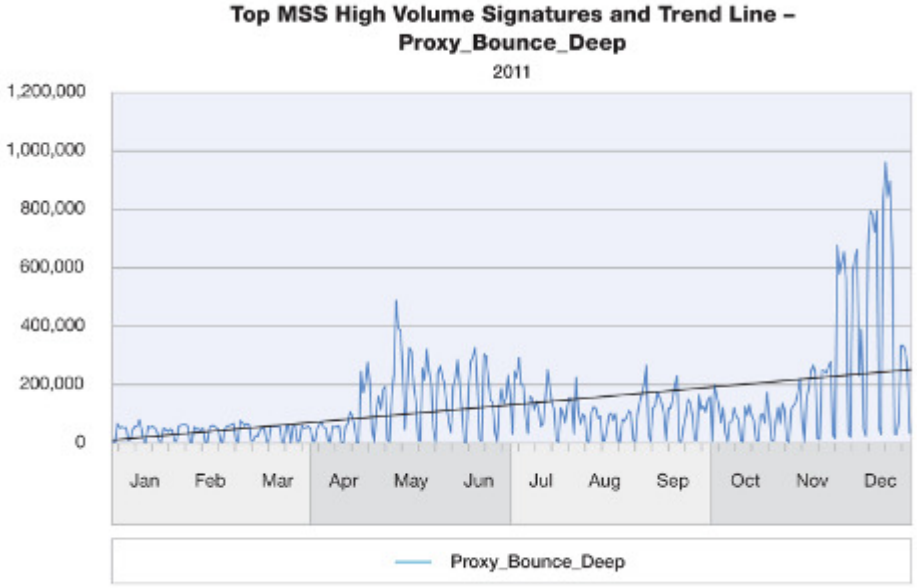
Anonymous proxies on the rise

- Approximately 4 times more anonymous proxies than seen 3 years ago
- Some used to hide attacks, others to evade censorship



Source: IBM X-Force® Research and Development

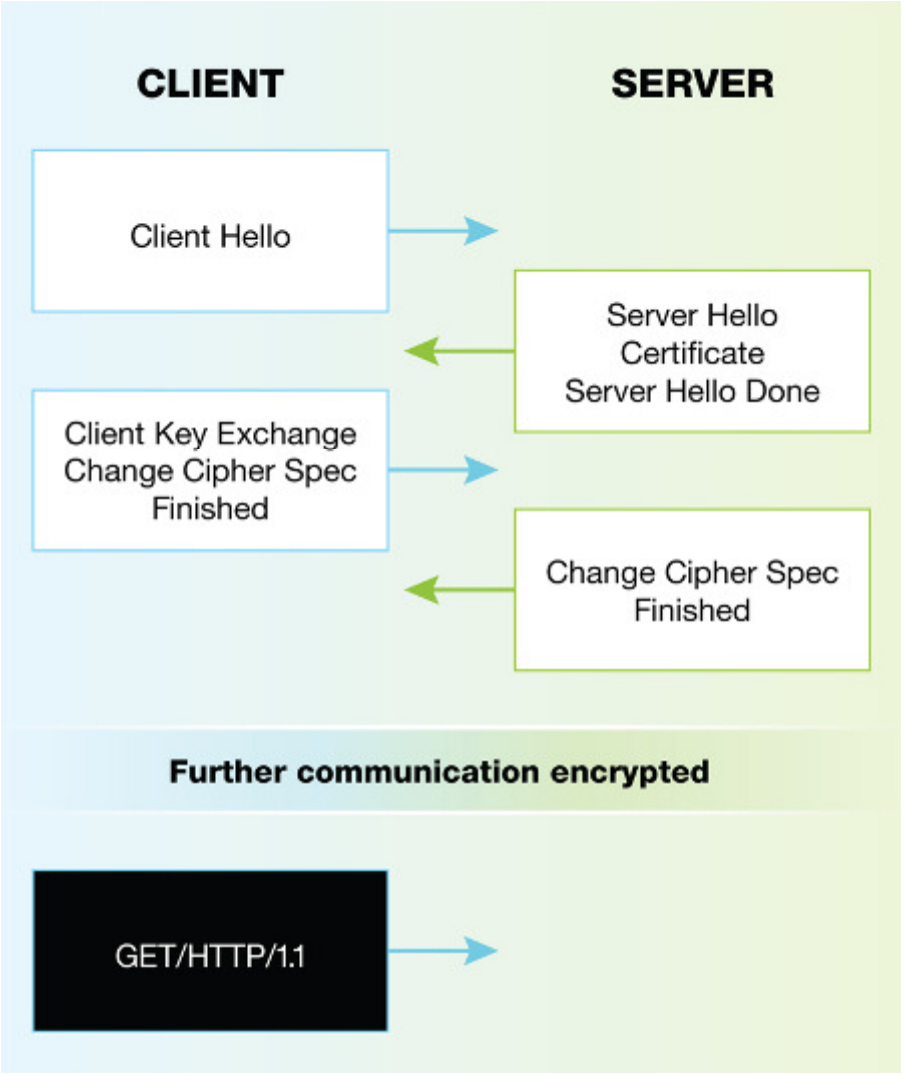
- Signature detects situations where clients are attempting to access websites through a chain of HTTP proxies
- Could represent
  - legitimate (paranoid) web surfing
  - attackers obfuscating the source address of launched attacks against web servers



Source: IBM X-Force® Research and Development

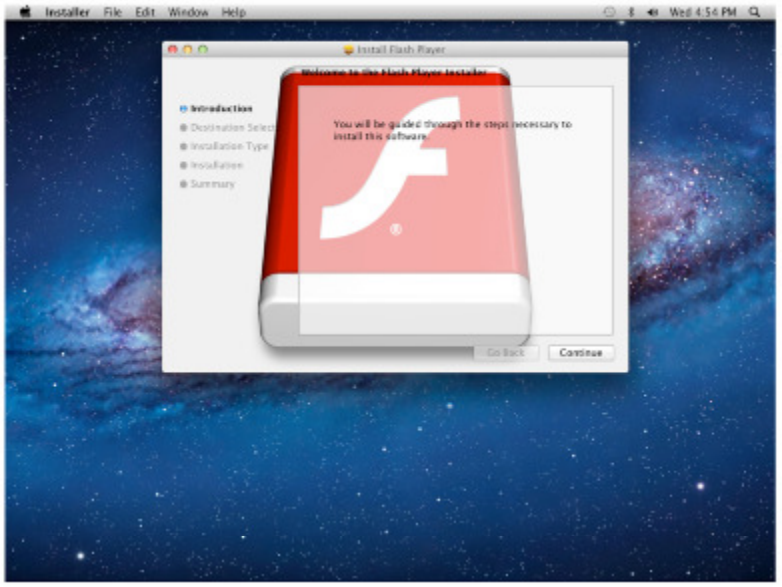
Challenges to SSL security

- Attackers able to generate unauthorized certificates for later interception using man-in-the-middle types of attacks
  - Used to attempt to listen in on encrypted connections
  - Breaks a basic trust for users—that visiting encrypted SSL pages mean communicating securely
- THC SSL-DOS
  - Proof-of-concept tool used to perform denial-of-service (DoS) attack against servers communicating via SSL/TLS
  - Potential for everyday laptop on average connection to take down an enterprise web server



MAC malware

- 2011 has seen the most activity in the Mac malware world.
  - Not only in volume compared to previous years, but also in functionality.
- In 2011, we started seeing Mac malware with functionalities that we've only seen before in Windows® malware.



Source: IBM X-Force® Research and Development

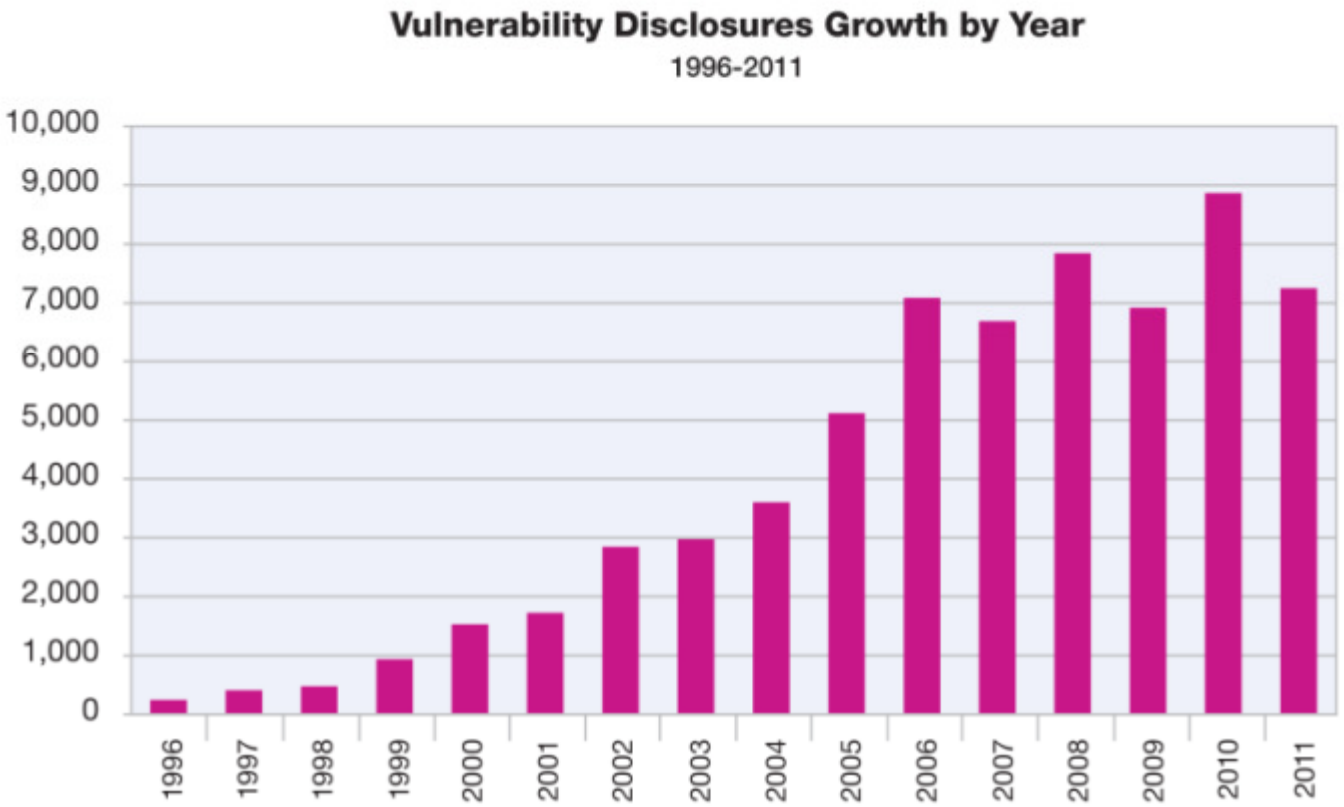
Source: IBM X-Force® Research and Development

Key Messages from the 2011 Trend Report

- New Attack Activity
  - –Rise in Shell Command Injection attacks
  - – Spikes in SSH Brute Forcing
  - – Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - – Fewer exploit releases
  - – Fewer web application vulnerabilities
  - – Better patching
- The Challenge of Mobile and the Cloud
  - – Mobile exploit disclosures up
  - – Cloud requires new thinking
  - – Social Networking no longer fringe pastime

Vulnerability disclosures down in 2011

- Total number of vulnerabilities decline — but it's cyclical
  - We have witnessed a two year, high-low cycle in vulnerability disclosures since 2006



Source: IBM X-Force® Research and Development

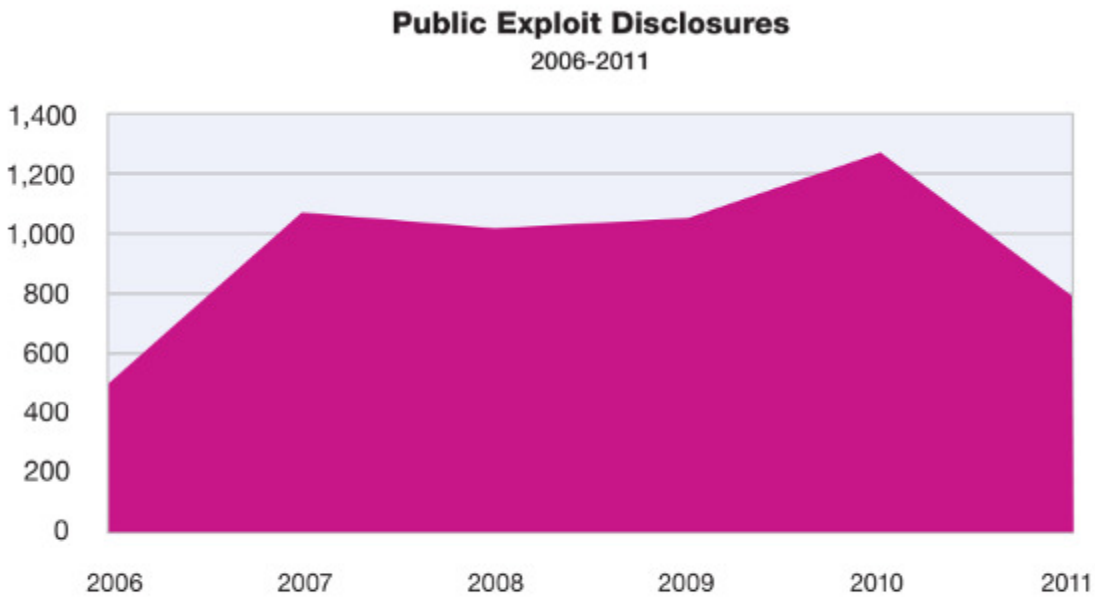
Challenging exploits: more vulnerabilities in widespread category

- 34 X-Force alerts and advisories in 2011
  - 16 fit the critical category
    - easy to exploit, sweet spot for malicious activity
    - most currently being exploited in the wild
  - 12 harder to exploit but high value
    - This number higher than previous years

Source: IBM X-Force® Research and Development

Public exploit disclosures

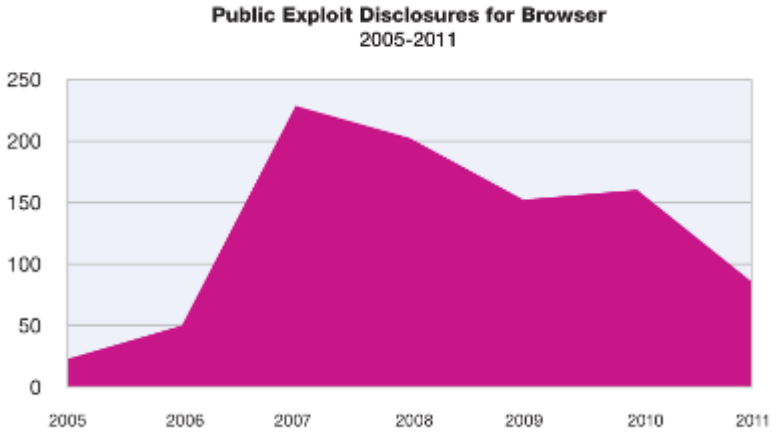
- Total number of exploit releases down to a number not seen since 2006
  - Also down as a percentage of vulnerabilities



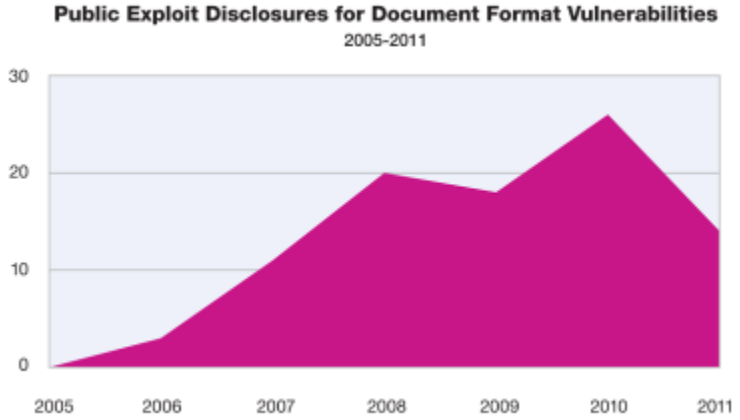
	2006	2007	2008	2009	2010	2011
Public Exploits	504	1078	1025	1059	1280	778
Percentage of Total	7.3%	16.5%	13.3%	15.6%	14.7%	11.0%

Source: IBM X-Force® Research and Development

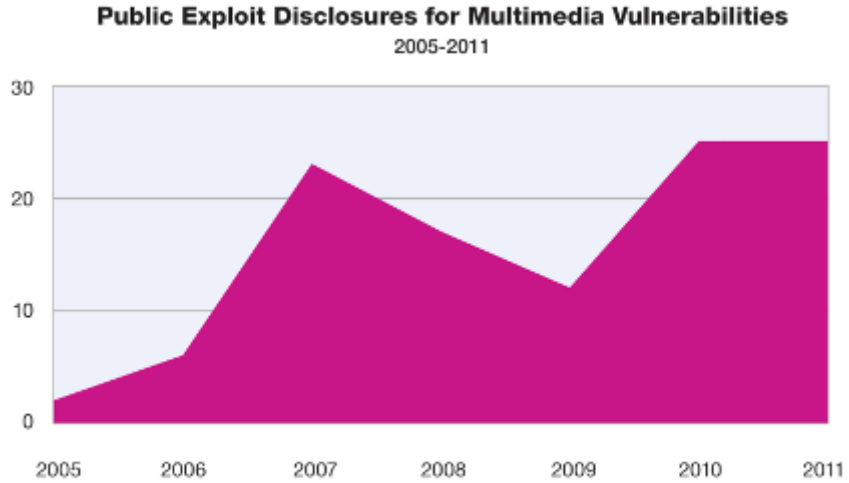
Public exploits



Source: IBM X-Force® Research and Development

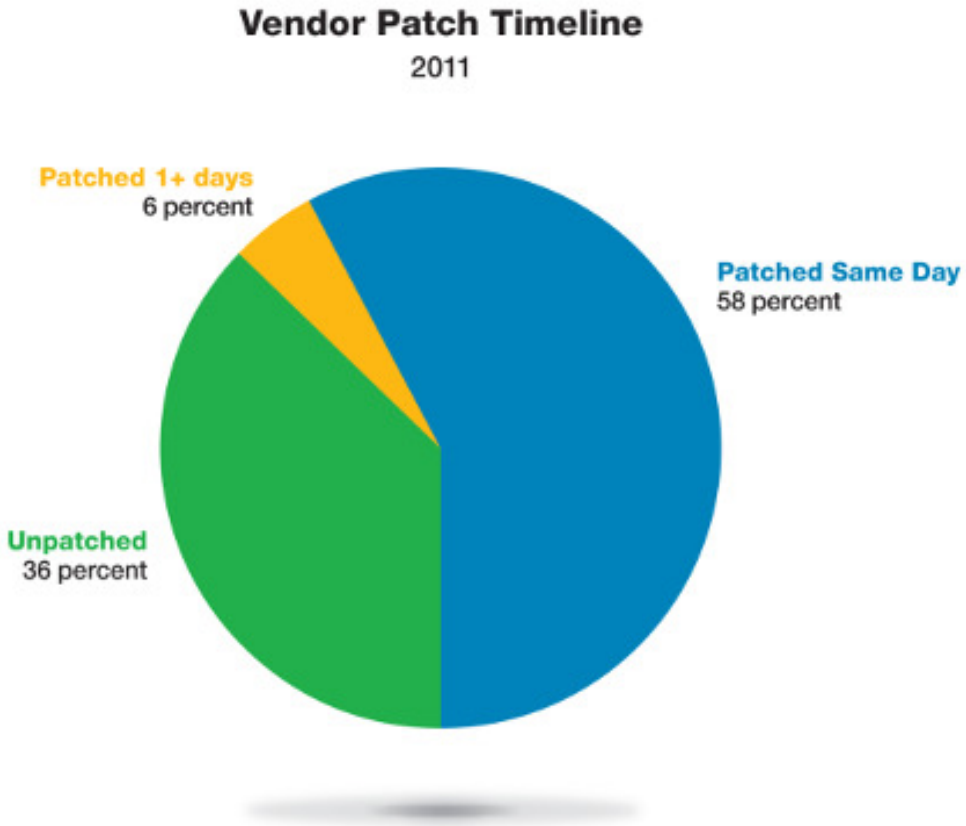


Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Better patching

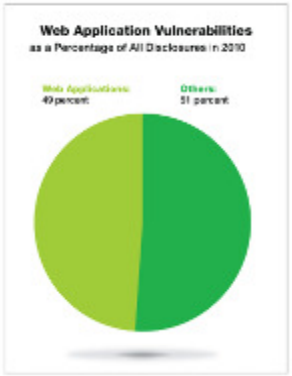


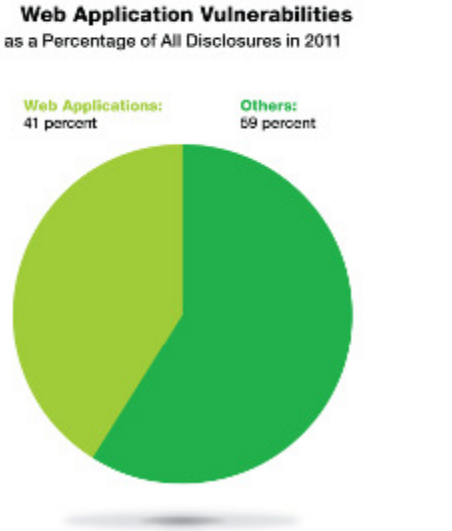
	2006	2007	2008	2009	2010	2011
Unpatched %	46.6%	44.6%	51.9%	45.1%	43.3%	36.0%

Source: IBM X-Force® Research and Development

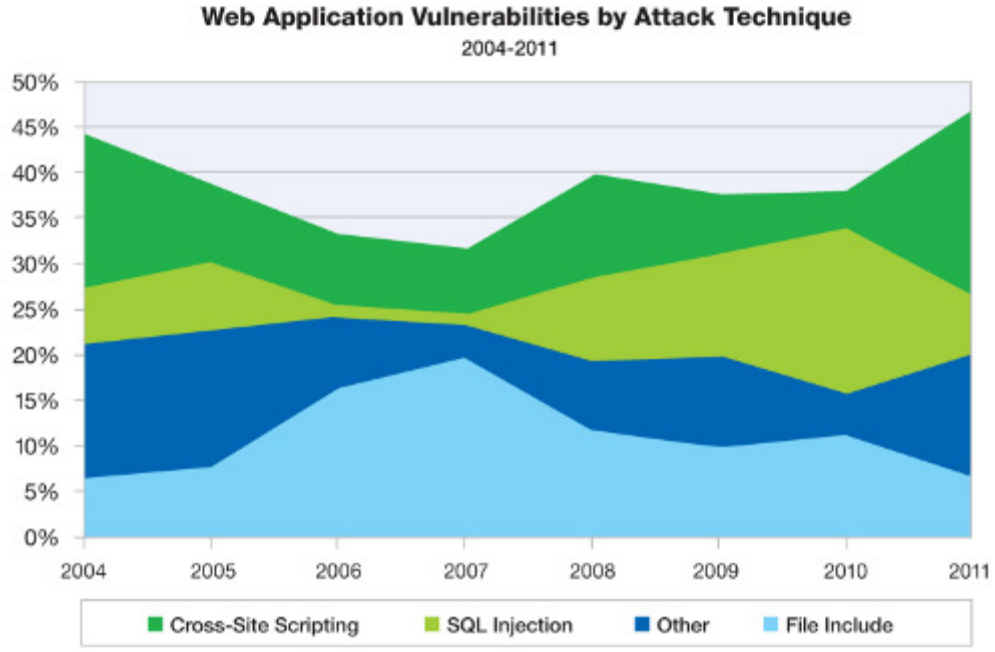
Decline in web application vulnerabilities

- In 2011, 41% of security vulnerabilities affected web applications
  - Down from 49% in 2010
  - Lowest percentage seen since 2005





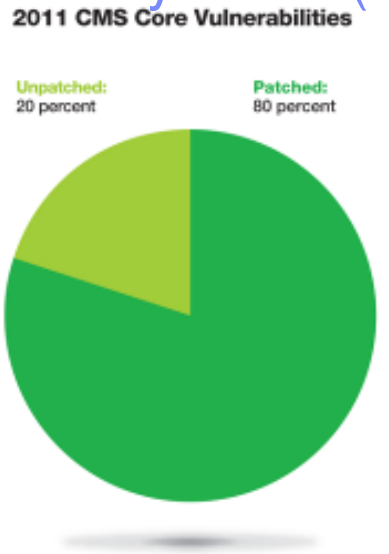
Source: IBM X-Force® Research and Development

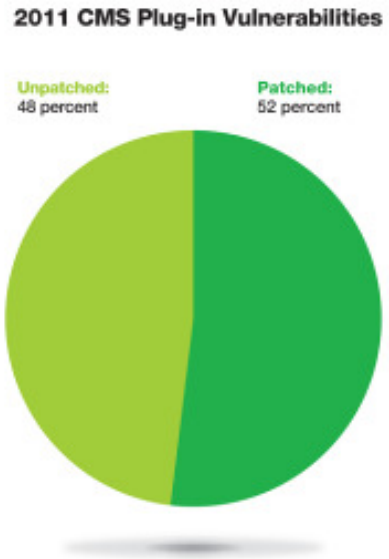


Source: IBM X-Force® Research and Development

Attack activity in web-based content management systems (CMS)

- Web CMS vulnerabilities are favorite targets of attackers because they are publicly disclosed and impact a large number of websites on the Internet.
  - Zero day vulnerabilities in these systems have factored into a number of breaches this year

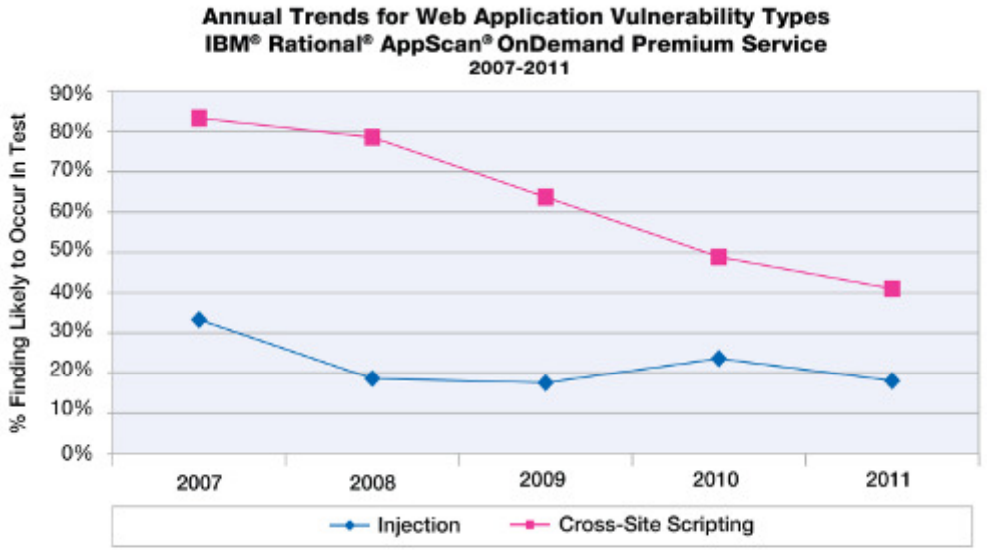




Source: IBM X-Force® Research and Development

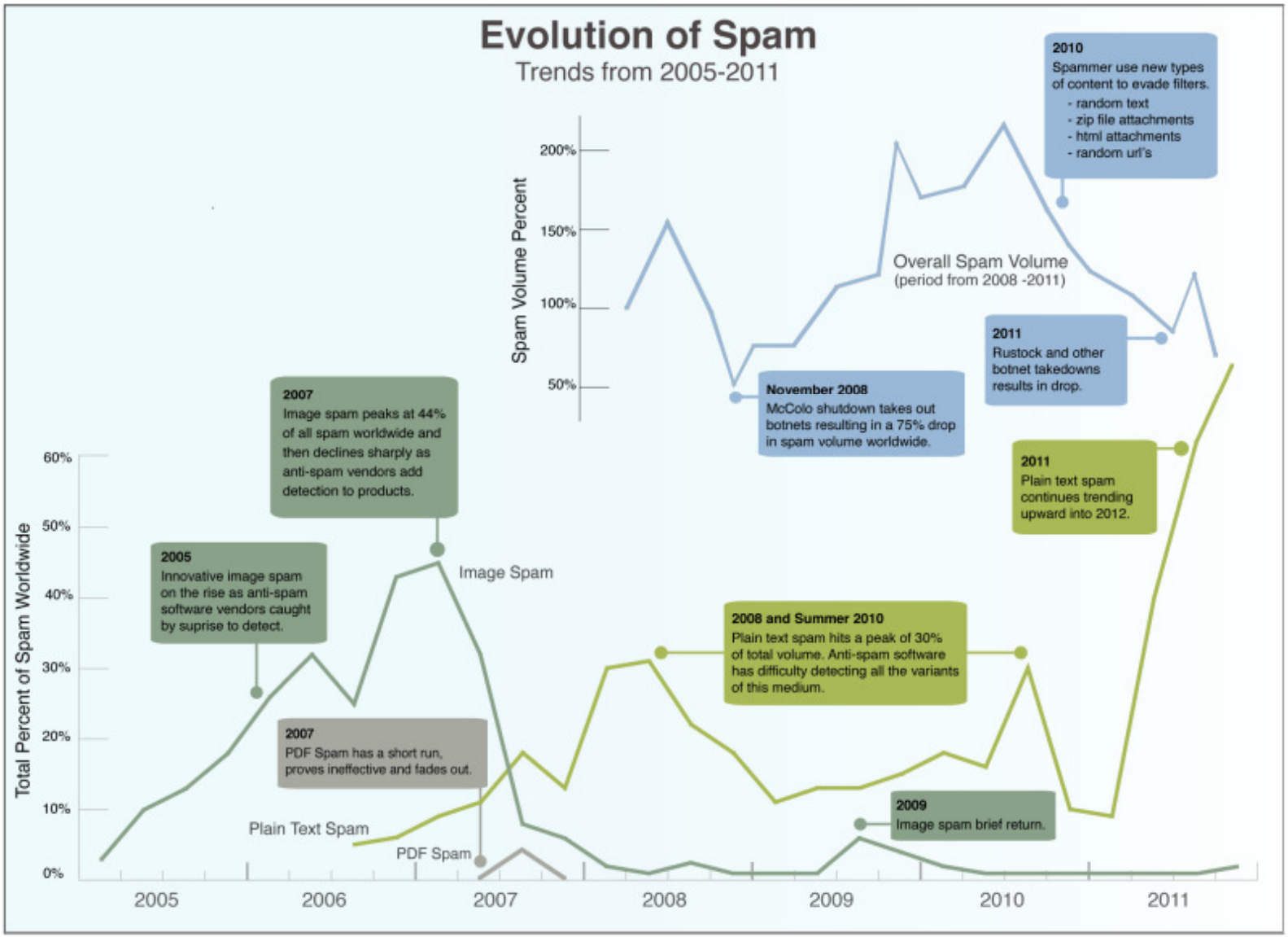
Cross Site Scripting (XSS) vulnerabilities

- In 2011 XSS vulnerabilities half as likely to exist in customer's as compared to 4 years ago
- However, XSS vulnerabilities still appear in about 40% of the applications IBM scans
  - High for something well understood and easily addressed



Source: IBM X-Force® Research and Development

Evolution of spam – trends from 2005 - 2011

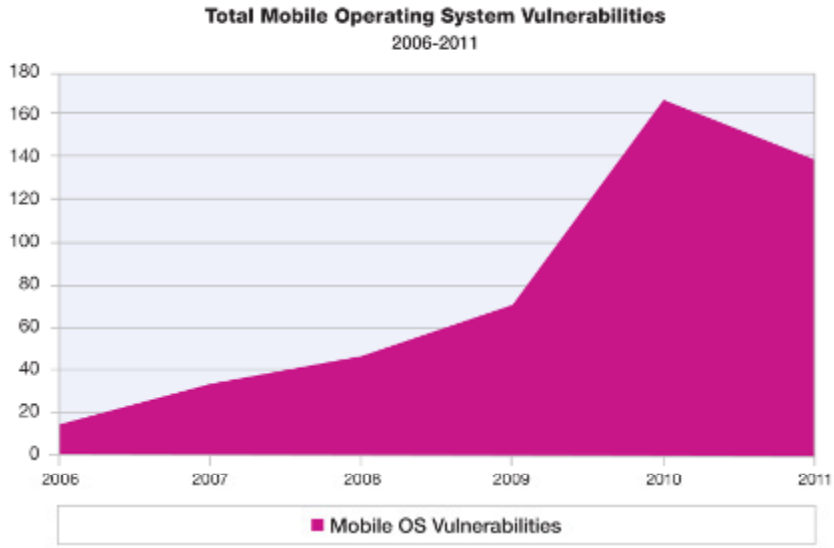


Key Messages from the 2011 Trend Report

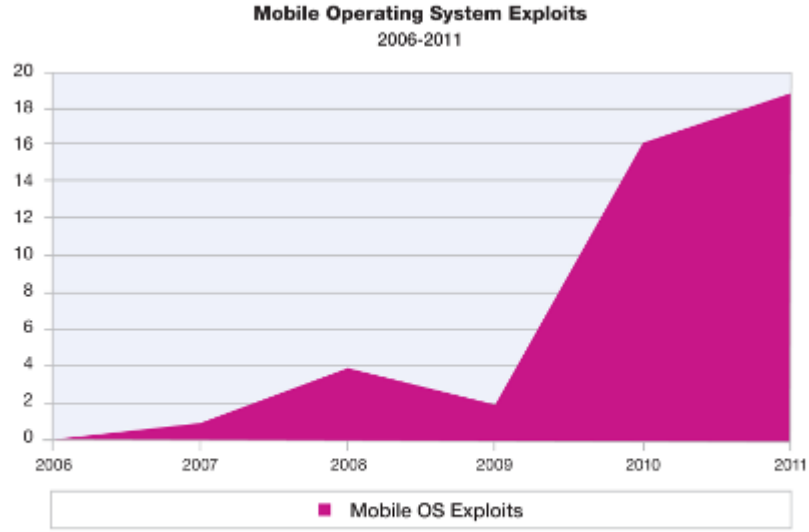
- New Attack Activity
  - –Rise in Shell Command Injection attacks
  - – Spikes in SSH Brute Forcing
  - – Rise in phishing based malware distribution and click fraud
- Progress in Internet Security
  - – Fewer exploit releases
  - – Fewer web application vulnerabilities
  - – Better patching
- The Challenge of Mobile and the Cloud
  - – Mobile exploit disclosures up
  - – Cloud requires new thinking
  - – Social Networking no longer fringe pastime

Mobile OS vulnerabilities & exploits

- Continued interest in Mobile vulnerabilities as enterprise users request a “bring your own device” (BYOD) strategy for the workplace



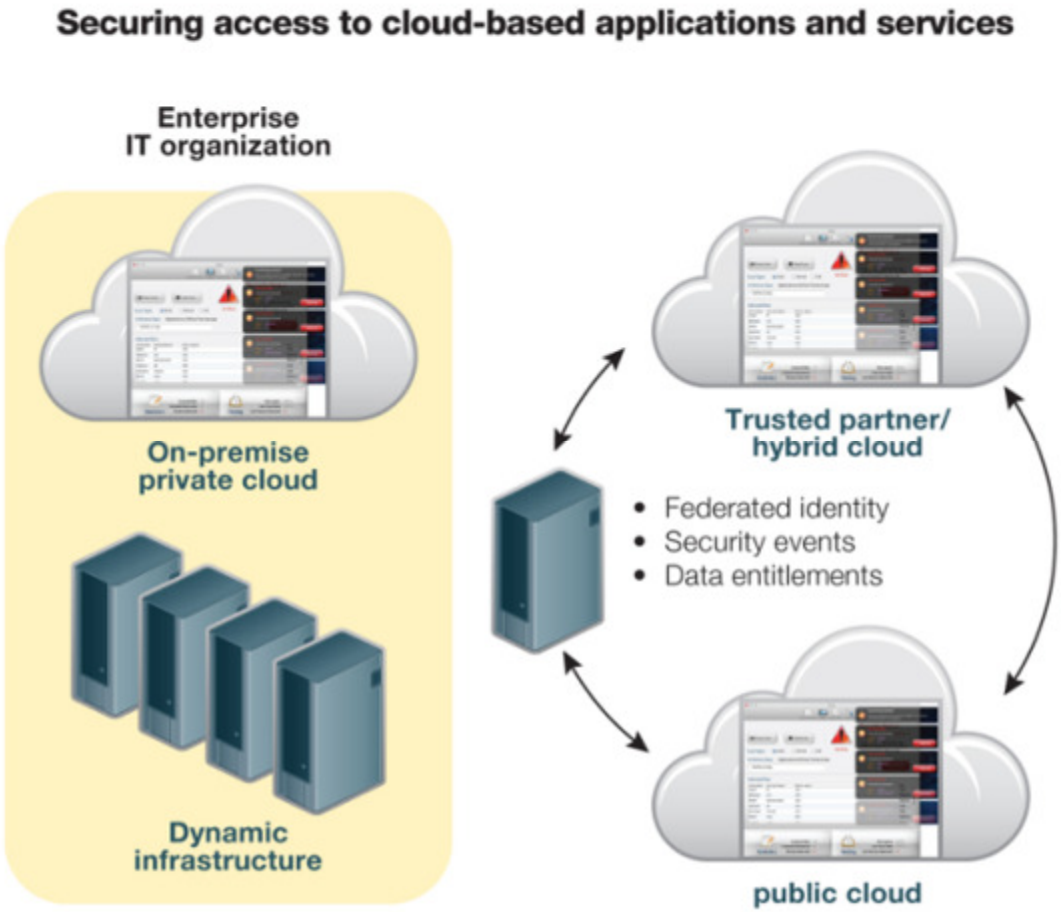
- Attackers finding these devices represent lucrative new attack opportunities



Source: IBM X-Force® Research and Development

Challenges of cloud security

- We saw a number of high profile cloud breaches in 2011 affecting well-known organizations and large populations of their customers
- Customers looking at cloud environments should consider:
  - Cloud-appropriate workloads
  - Appropriate service level agreements (SLAs)
  - Lifecycle approaches to deployment that include exit strategies should things not work out



Social Networking – no longer a fringe pastime

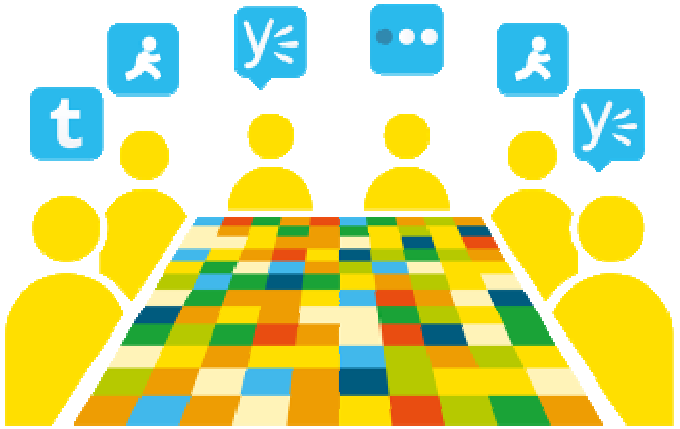
- Attackers finding social networks ripe with valuable information they can mine to build intelligence about organizations and its staff:
  - Scan corporate websites, Google, Google News
    - Who works there? What are their titles?
    - Create index cards with names and titles
  - Search Linkedin, Facebook, Twitter profiles
    - Who are their colleagues?
    - Start to build an org chart
  - Who works with the information the attacker would lik
    - What is their reporting structure?
    - Who are their friends?
    - What are they interested in?
    - What are their work/personal email addresses?

How to Address These Issues

Security Issue	Recommendations	IBM Security Systems Solutions
SQL injection attacks against web servers	Scan, identify and remediate vulnerabilities in web applications and software code; block attacks before updates are available	• AppScan • Network Intrusion Protection • InfoSphere Guardium Database Activity Monitor
Shell Command Injection attacks	Scan, identify and remediate vulnerabilities in web applications and software code; block attacks before updates are available	• AppScan • Network Intrusion Protection
SSH brute force activity	Search for and prevent the use of weak passwords; prevent the deployment of systems with default password onto the network	• Endpoint Manager • zSecure Audit • Network Intrusion Prevention • InfoSphere Guardium Database Vulnerability Assessment • Identity and Access Assurance
Phishing-based malware distribution & click fraud	Defend your network against spam and web based drive by download attacks	• Endpoint Manager • Network Intrusion Protection
Anonymous Proxies	Consider blocking proxied connections inbound to your web server depending on your security policies (this solution isn't for everyone)	• Access Manager for e-Business • InfoSphere Guardium Database Activity Monitor
Mobile Malware	Look to deploy mobile endpoint management solutions	• Endpoint Manager for Mobile Devices • Mobile Device Security in the Cloud (SaaS)

Now a business problem…

- Organizations are making security a strategic priority
  - Enabler of innovation and value, not just a cost of doing business
- Requiring fundamental changes in processes and attitudes
- Strategic shift needs a new breed of security leader
  - Clear voice in the C-suite and the power to drive meaningful change



IBM's own strategy: Ten essential practices for security leaders

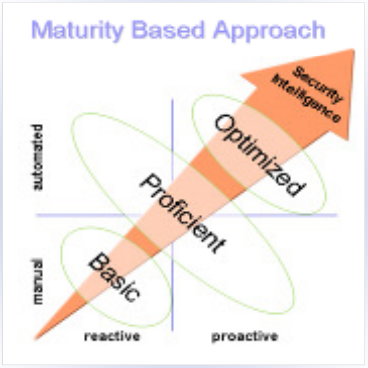
Kristin Lovejoy
IBM Vice President, IT Risk

5. Take a Hygienic Approach to Managing Infrastructure

6. Control Network Access

4. Secure Services, By Design

7. Address New Complexity of Cloud and Virtualization



3. Secure the Workplace of the Future (Endpoint)

8. Assure Supply Chain Security Compliance

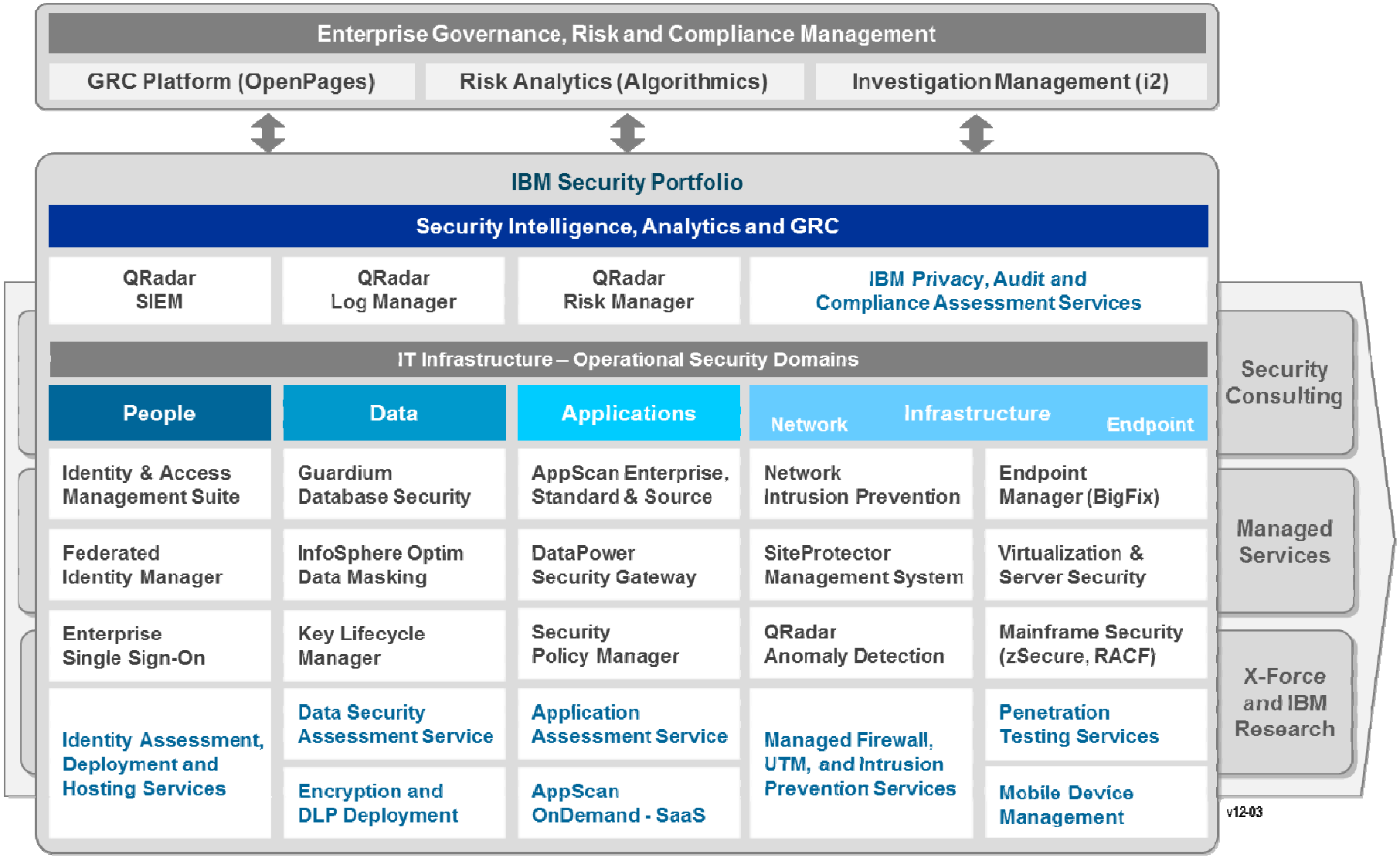
2. Manage Incidents

9. Protect Structured & Unstructured Data

1. Build a Risk Aware Culture & Management System

10. Manage the Identity Lifecycle

Intelligence: Leading products and services in every segment



Connect with IBM X-Force research & development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www.ibm.com/security/xforce

Subscribe to X-Force alerts at http://iss.net/rss.php or Frequency X at http://blogs.iss.net/rss.php

Attend in-person events

http://www.ibm.com/events/calendar/

Join the Institute for Advanced Security

www.instituteforadvancedsecurity.com

Subscribe to the security channel for latest security videos

www.youtube.com/ibmsecuritysolutions

ibm.com/security