

Security Intelligence.
Think Integrated.

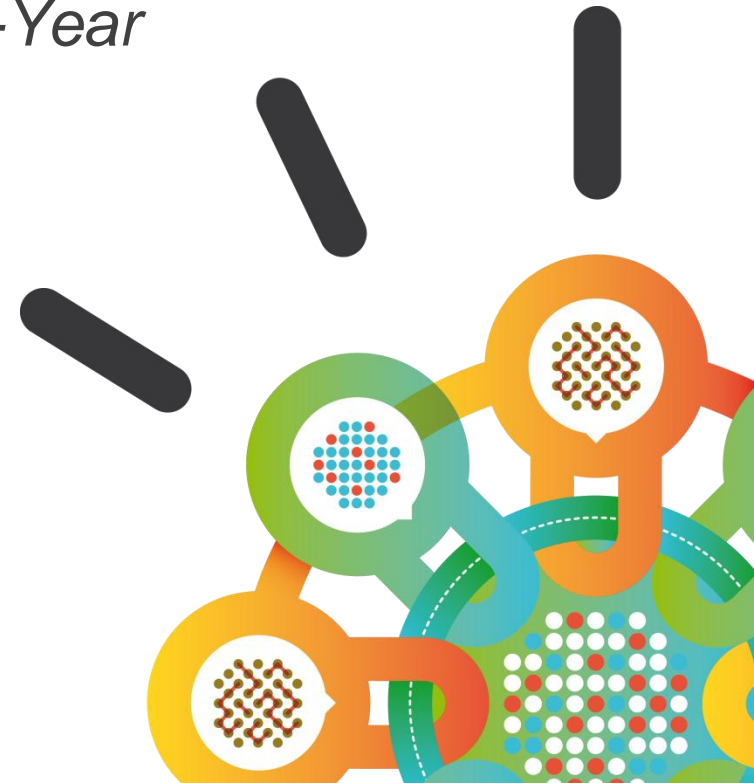
IBM X-Force – Trending the Threat

*Data and Research from the 2012 Mid-Year
Trend & Risk report*

Leslie Horacek

X-Force Threat Response Manager

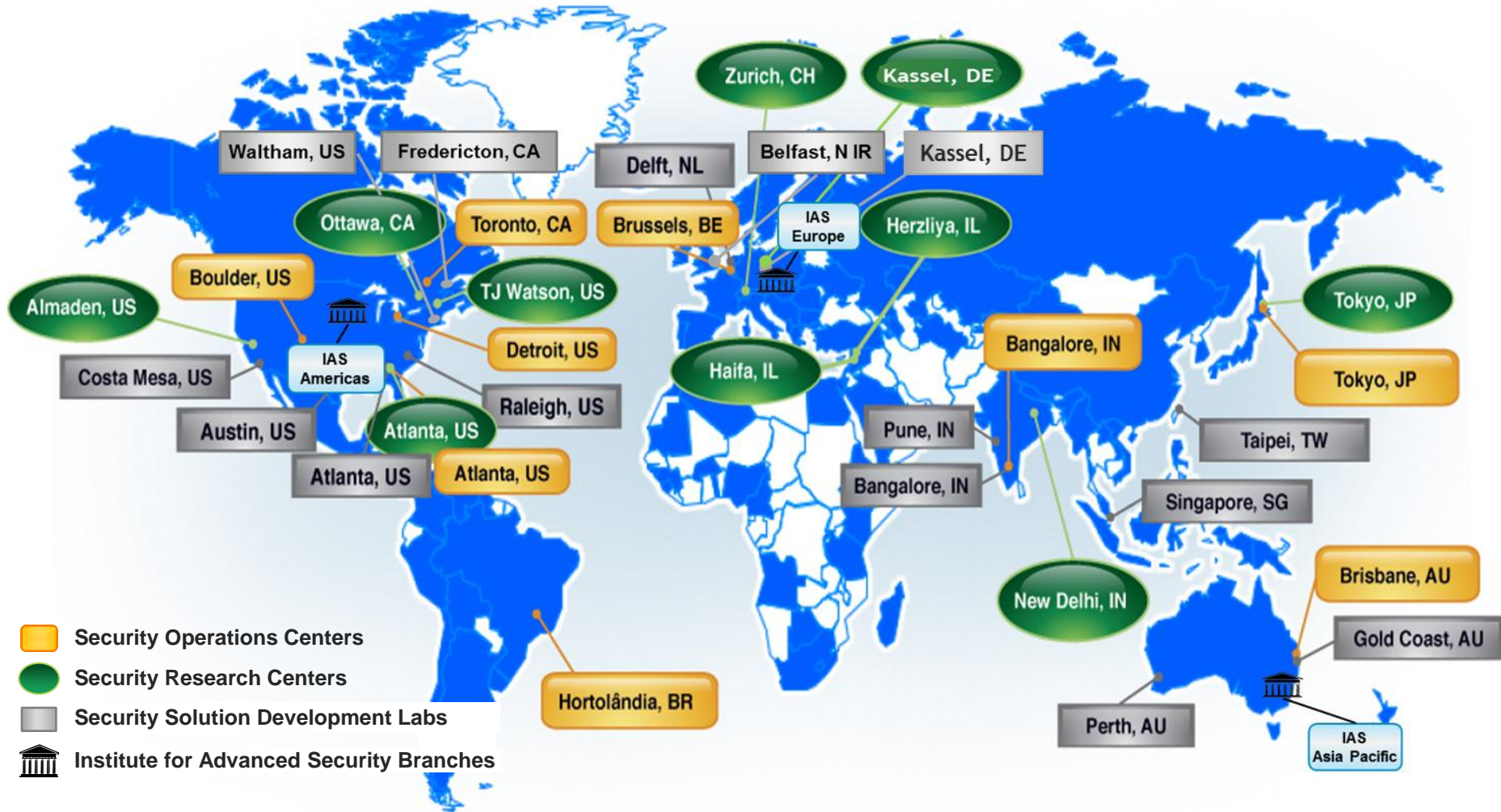
January 2013





The Cyber Landscape

At IBM, the world is our Security lab



15,000 researchers, developers and subject matter experts
working security initiatives worldwide

Collaborative IBM teams monitor and analyze the latest threats

Coverage

20,000+ devices
under contract

3,700+ managed
clients worldwide

13B+ events
managed per day

133 monitored
countries (MSS)

1,000+ security
related patents



IBM Research

Depth

14B analyzed
web pages & images

40M spam &
phishing attacks

64K documented
vulnerabilities

Billions of intrusion
attempts daily

Millions of unique
malware samples

What are we seeing?

**Annual report
gives a view of
changes in the
threat landscape**

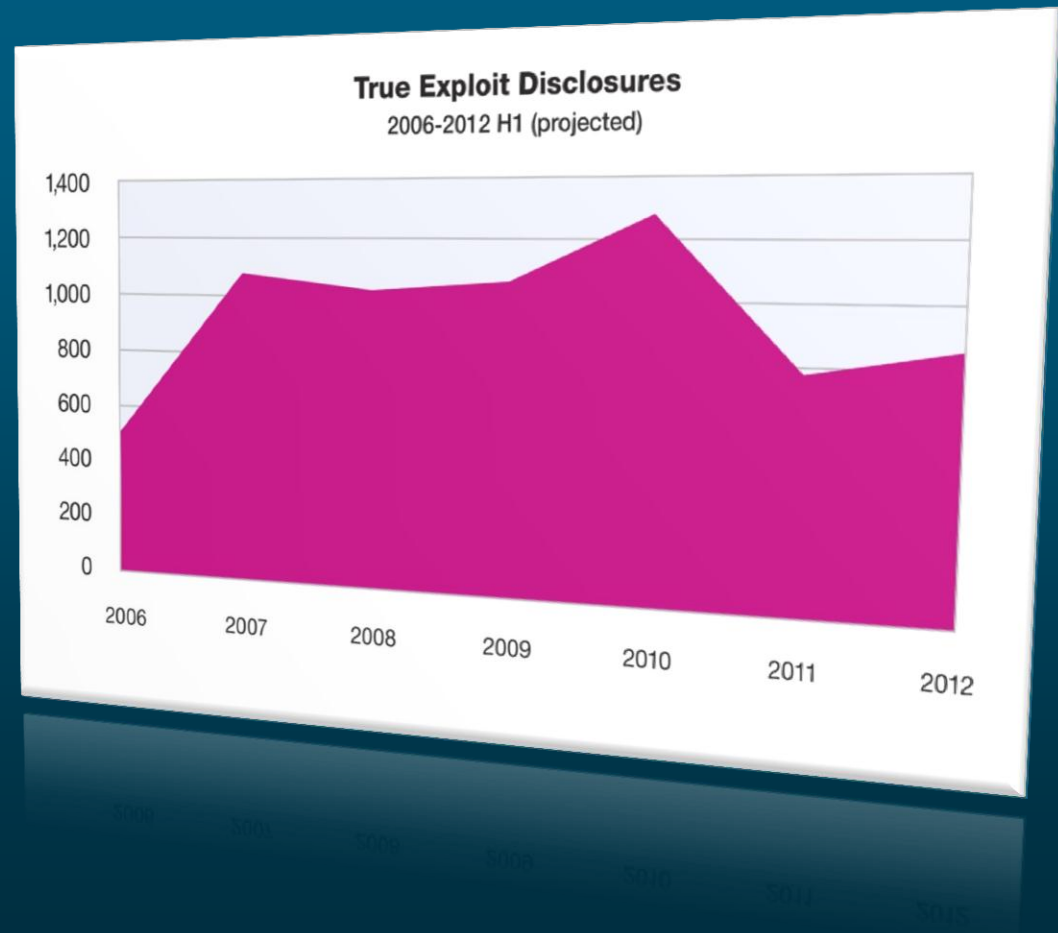
Key findings...



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Fewer
public exploit
disclosures
as a % of total
vulnerabilities

Is software
harder to exploit?



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Success in
sandboxing

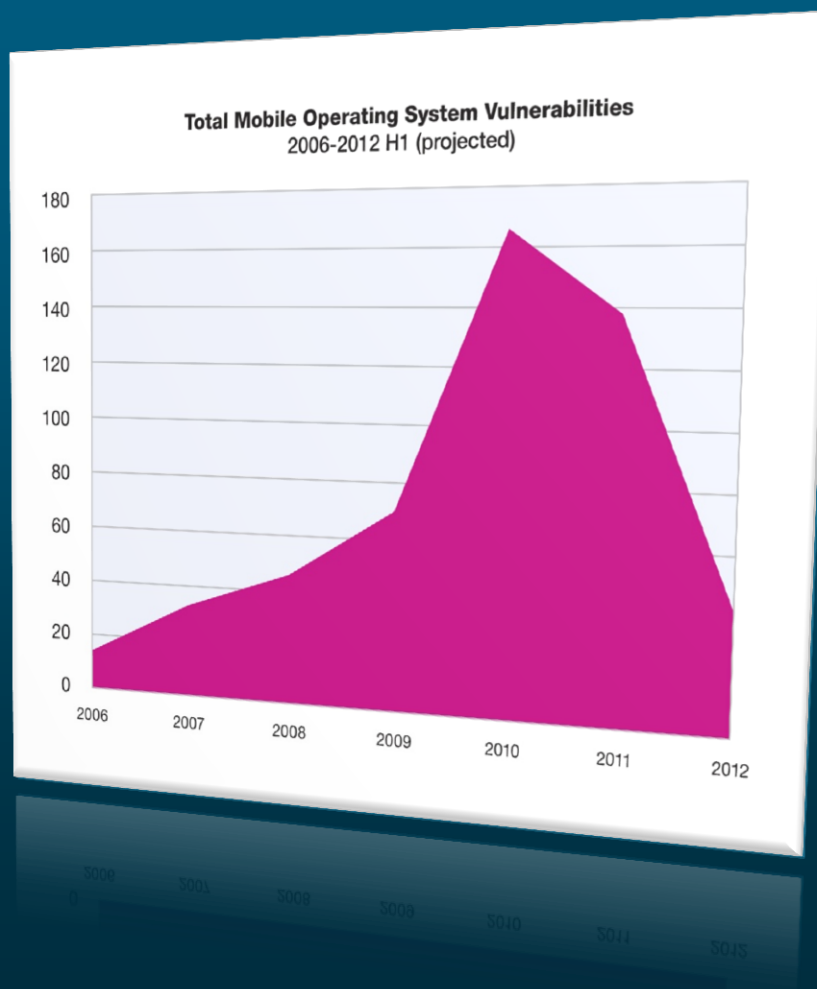
Significant
decrease
in PDF
vulnerabilities



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Surprise!
Fewer mobile
operating
system
vulnerabilities
disclosed in
H1 2012

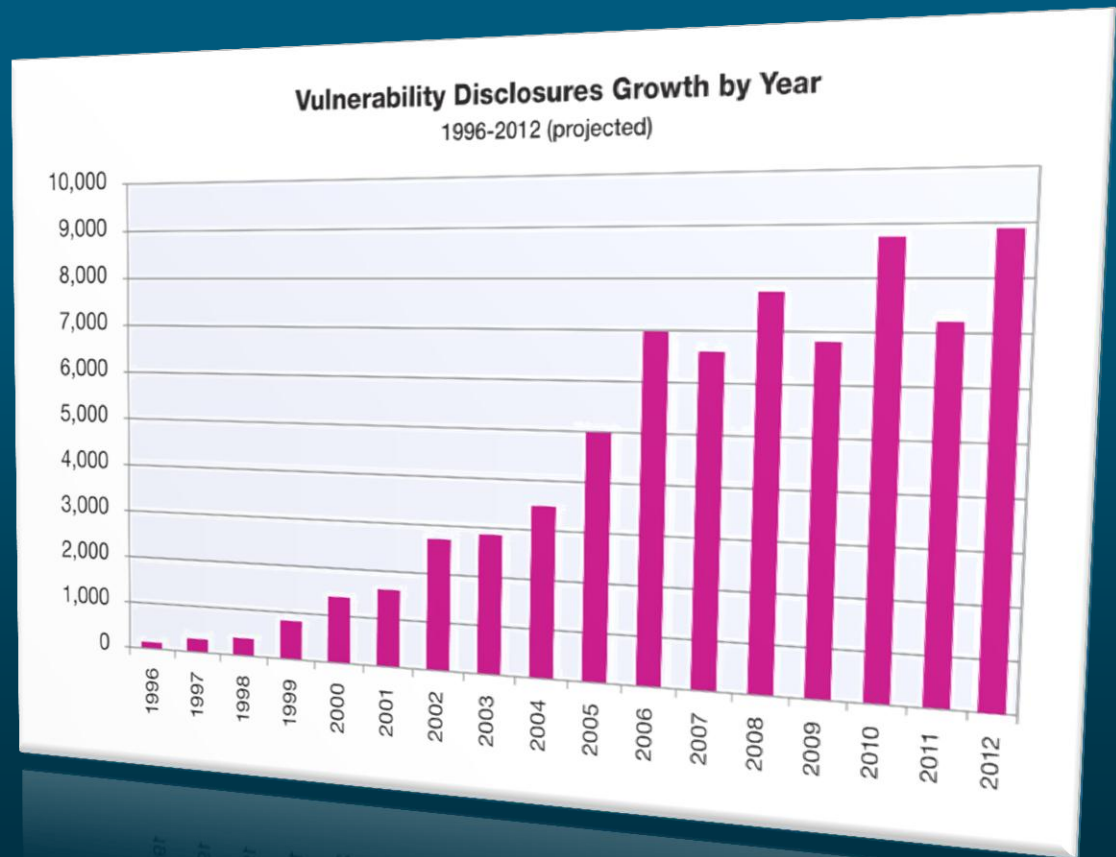
But...



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Vulnerability disclosures up in 2012

4,400
in 1H 2012
(on track for a record year)



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

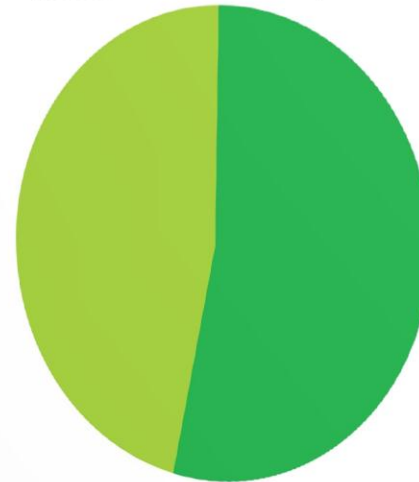
Web Application Vulnerabilities Rise Again

47% of all vulnerabilities affect web applications

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2012 H1

Web Applications:
47 percent

Others:
53 percent



What is the difference between XSS and SQLi ??

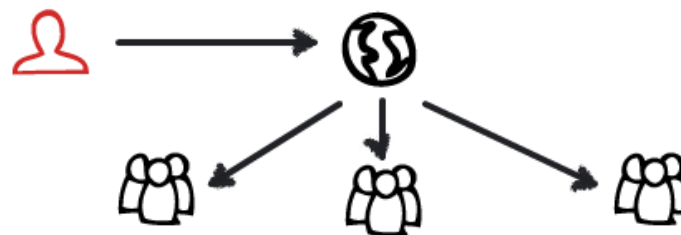
SQL Injection

vs.

Cross Site Scripting (XSS)

User:

Password:



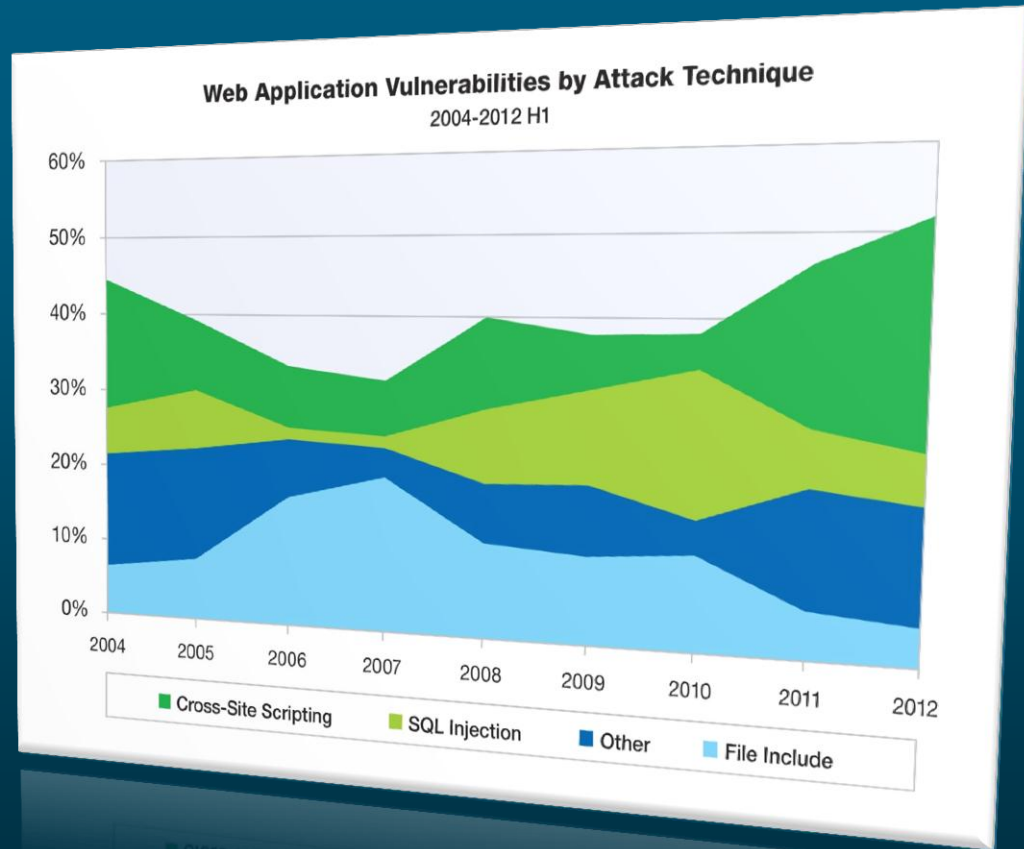
- SQL injection (in base terms) is when an attacker goes after a database to take information.
- XSS (in base terms) is when an attacker attempts to “redirect” users from one site to another malicious site

Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Cross Site Scripting reaches an all time high

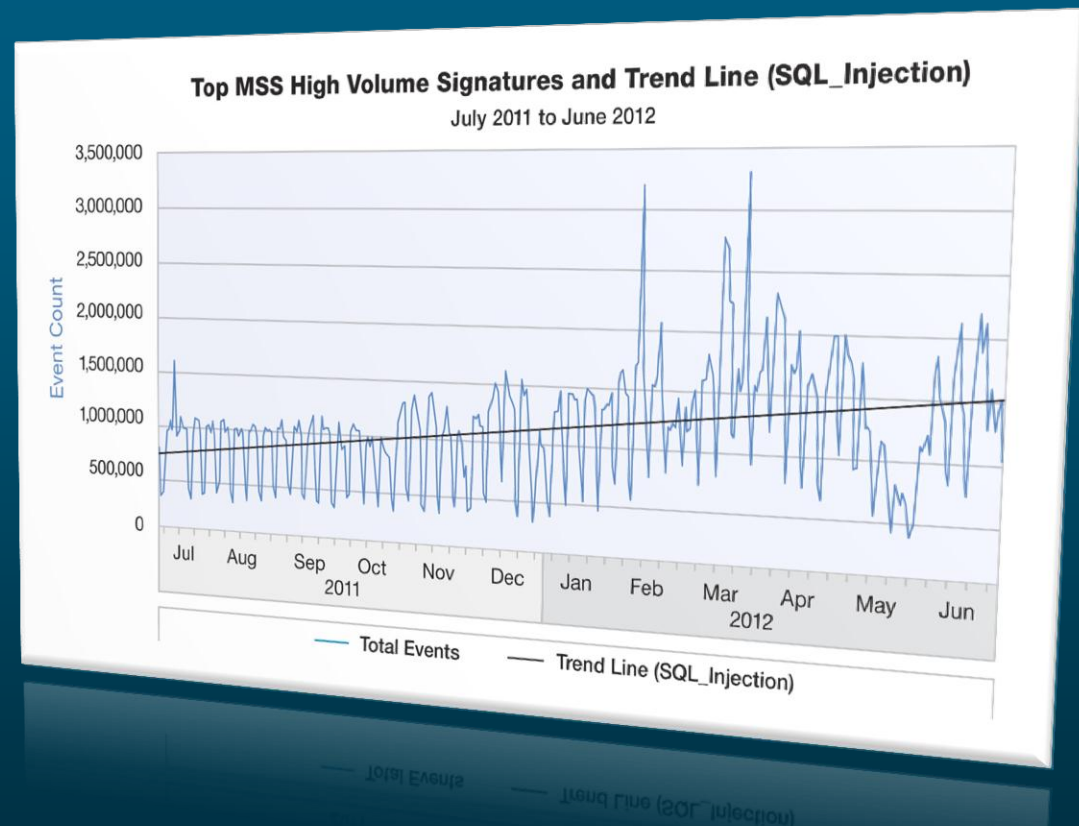
51%

are categorized as XSS



Findings from the 2012 X-Force® Mid Year Trend and Risk Report

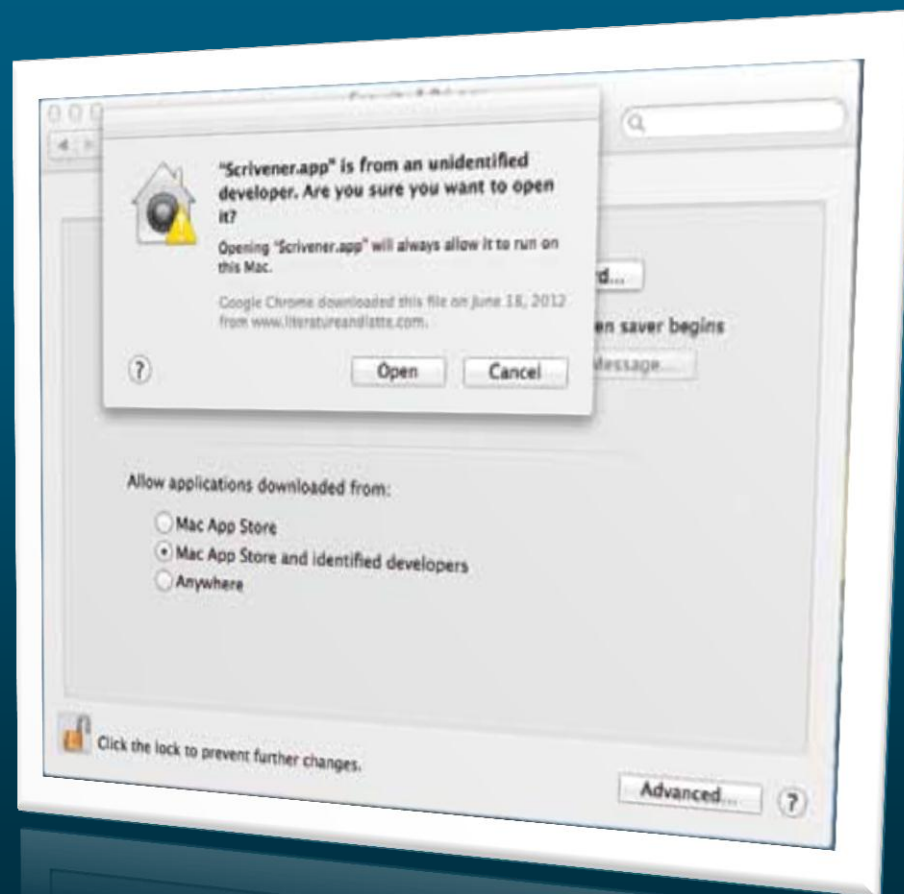
**SQL
Injection
activity
reversed in
2011 and
continues to
increase**



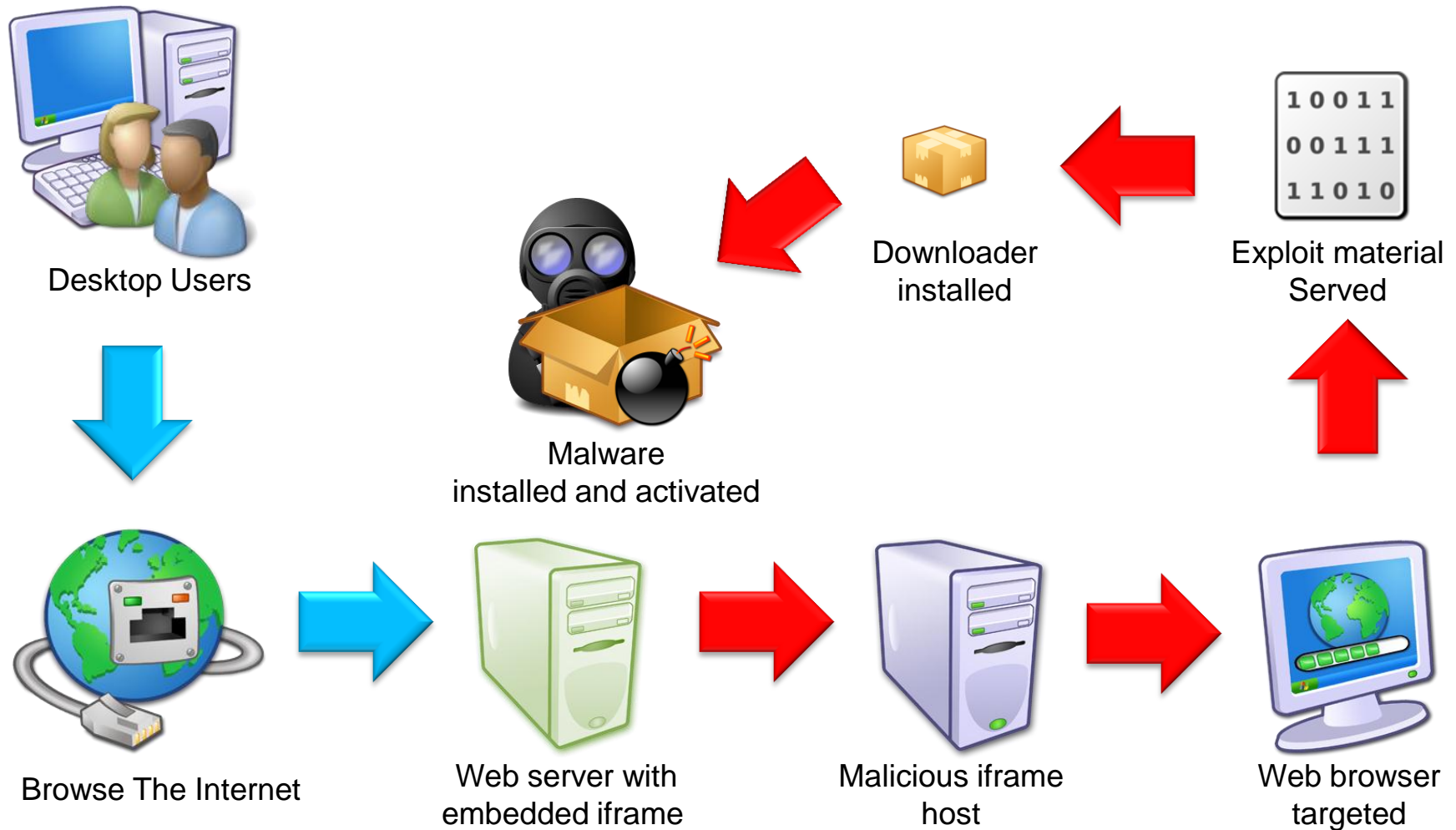
Findings from the 2012 X-Force® Mid Year Trend and Risk Report

Developments in Mac Malware

Flashback
outbreak and the
discovery of
advanced
persistent threat
(APT) Mac malware.



The drive-by-download process



Motivations and sophistication are rapidly evolving

**National
Security**



Nation-state
actors
Stuxnet

**Espionage,
Activism**



Competitors and
Hacktivists
Aurora

**Monetary
Gain**



Organized
crime
Zeus

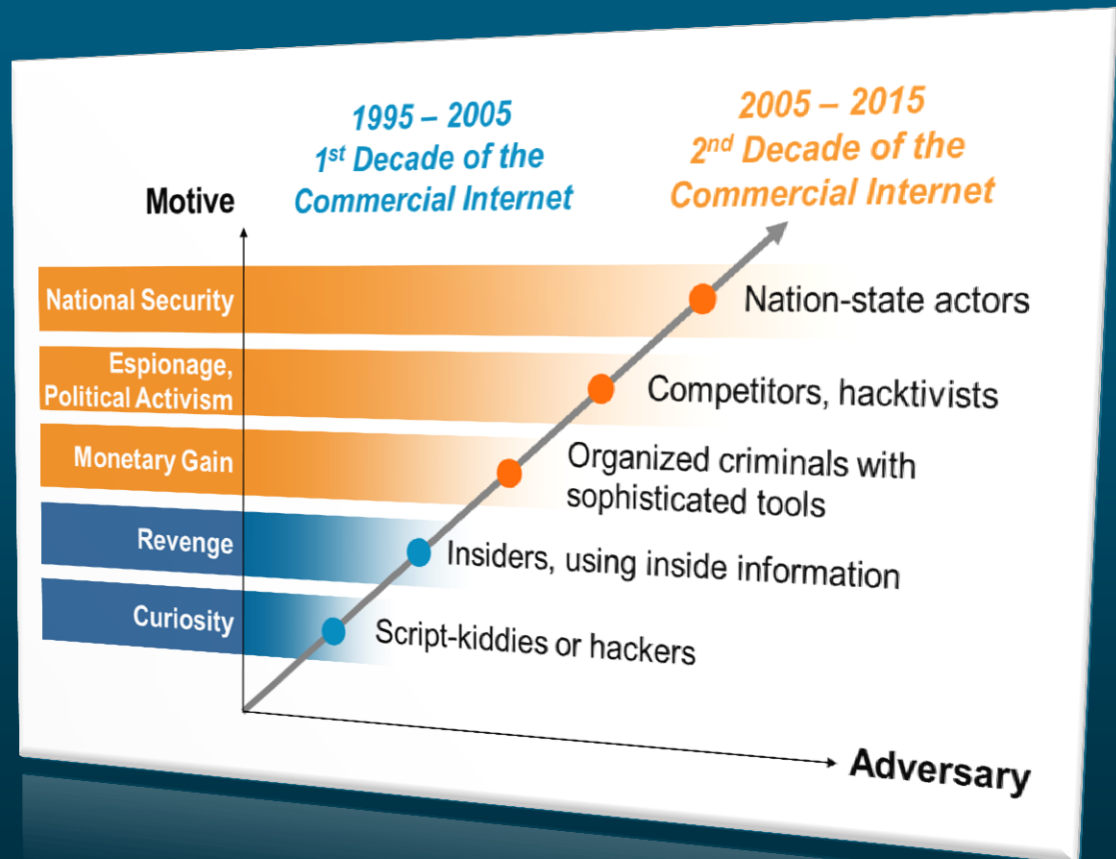
**Revenge,
Curiosity**



Insiders and
Script-kiddies
Code Red

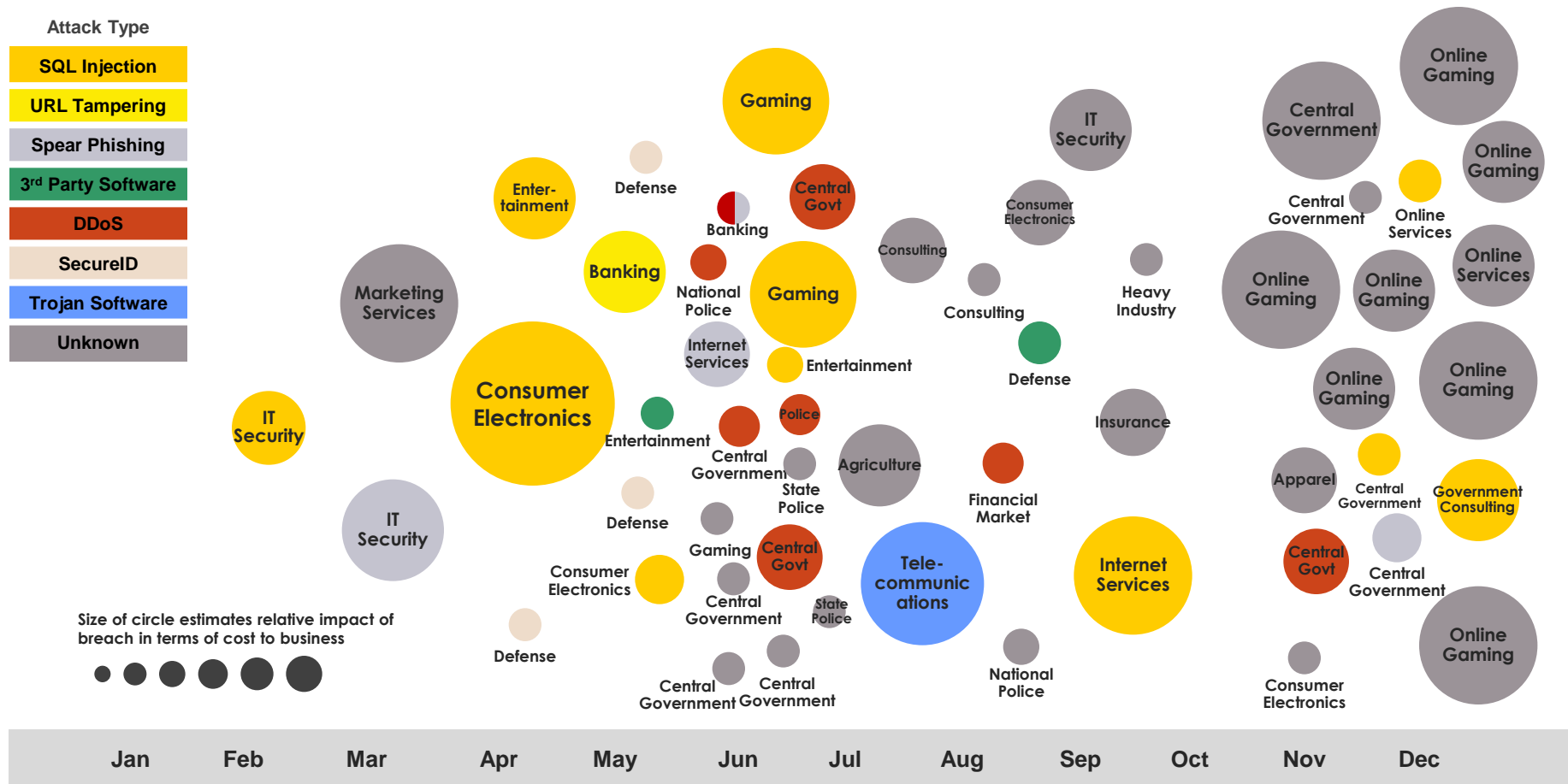
Motivation and sophistication is evolving rapidly

- Attackers have more resources
- Off-the-shelf tools are available for sale
- They will keep trying until they get in



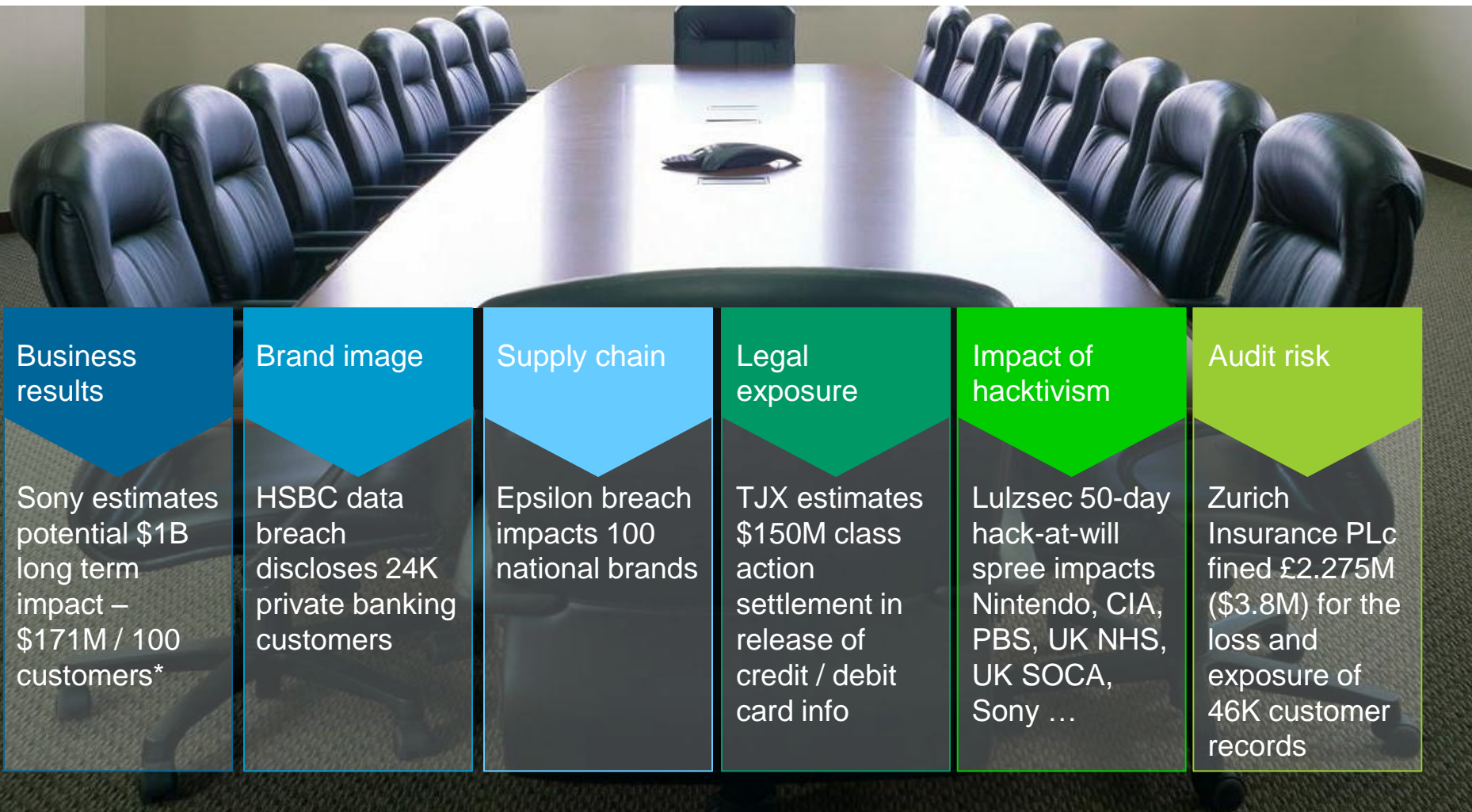
Nobody is immune

2011 Sampling of Security Incidents by Attack Type, Time and Impact



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

IT Security is a board room discussion



Business results

Sony estimates potential \$1B long term impact – \$171M / 100 customers*

Brand image

HSBC data breach discloses 24K private banking customers

Supply chain

Epsilon breach impacts 100 national brands

Legal exposure

TJX estimates \$150M class action settlement in release of credit / debit card info

Impact of hacktivism

Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony ...

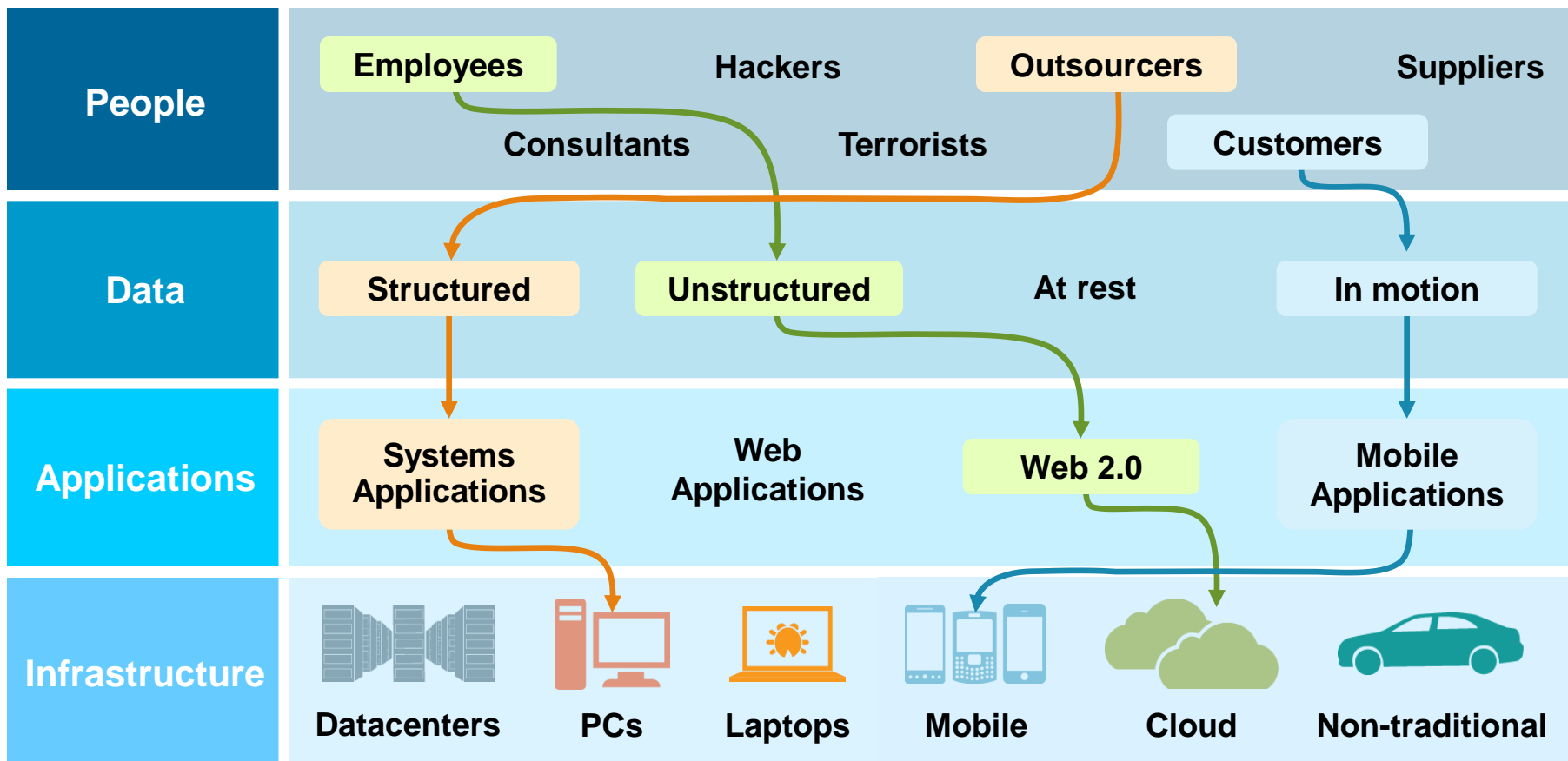
Audit risk

Zurich Insurance PLC fined £2.275M (\$3.8M) for the loss and exposure of 46K customer records



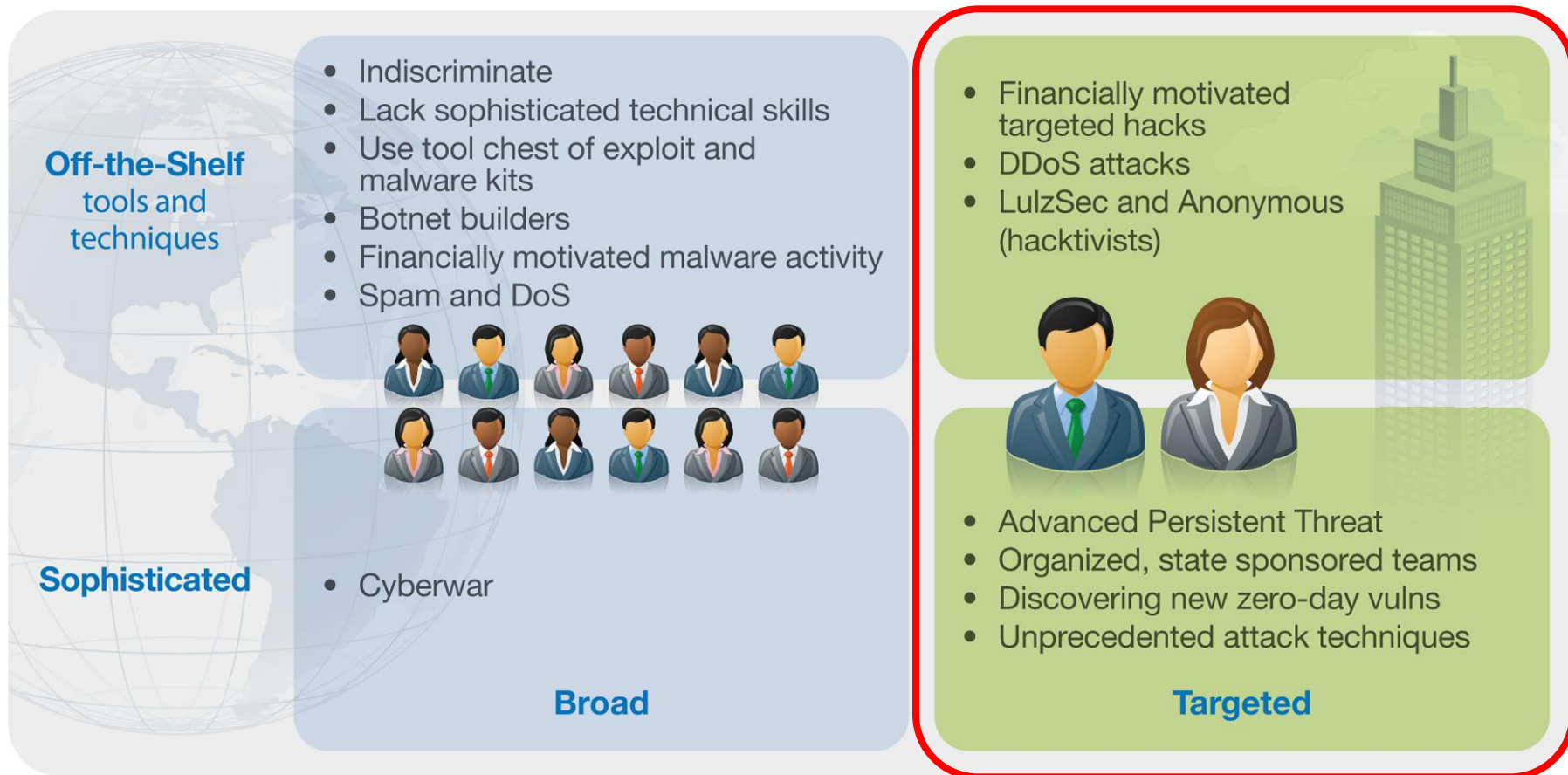
The Security Challenge

Solving a security issue is a complex, four-dimensional puzzle



Attempting to protect the perimeter is not enough – siloed point products and traditional defenses cannot adequately secure the enterprise

Attackers are using sophisticated techniques to bypass defenses



Source: IBM X-Force® Research and Development



CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data is disappearing.



Mobile is the next evolution in computing

Employees

34%

employees in 2012 are mobile
(Source: IDC*)

Mobile/Wireless/Cloud

Web/Desktop

Client/Server

Host/Mainframe

Mobile Applications

85 billion

mobile applications will be
downloaded in 2012

(Source: IDC)

Security

8X

increase in security risk
driven by proliferation of
mobile data and devices

“Consumerisation of IT”

62%

individual-liable (BYOD*) devices used for
business, compared to 38% corporate-liable
in 2012

(Source: IDC*)

Unified Communications (UC)

78%

of multinational corporations plan to adopt
mobile UC by 2015, including mobile video
streaming and conferencing

Uniqueness of Mobile...

Mobile Devices are Shared More Often

Smartphones and tablets are multi-purpose personal devices. Therefore, users share them with friends, and family more often than traditional computing devices – laptops and desktops. Social norms on privacy are different when accessing file-systems vs. mobile apps



Mobile Devices are Used in More Locations

Smartphones and tablets are frequently used in challenging wireless situations that contrast with laptop friendly remote access centers. Laptops are used in a limited number of trusted locations



Mobile Devices prioritize User Experience

Smartphones and tablets place a premium on user experience and any security protocol that diminishes the experiences will not be adopted or will be circumvented. Workstation level security cannot be assumed unless they are dedicated devices



Mobile Devices have multiple personas

Smartphones and tablets may have multiple personas – entertainment device, work tool, etc. Each persona is used in a different context. Users may want to employ a different security model for each persona without affecting another.



Mobile Devices are Diverse

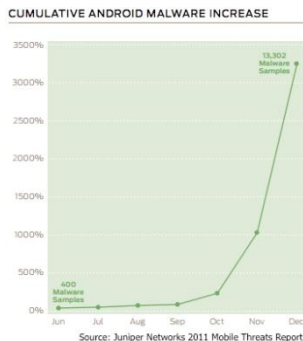
Smartphones and tablets employ a variety of different platforms and have numerous applications aimed at pushing the boundaries of collaboration. The standard interaction paradigms used on laptops and desktops cannot be assumed.



Mobile Security Threat Landscape

Malware

- Malware existed in various forms (viruses, worms, Trojans, spyware) has been constantly increasing.
- 25,000 mobile malware apps were identified as of the second quarter of 2012--a 417 percent rise from the first quarter. (Trend)



- No platform is immune. Malicious applications on increase in all app stores
- “Zeus for Mobile”
- First large scale mobile botnet in 1Q2012 – RootStrap (Symantec)

Loss and Theft

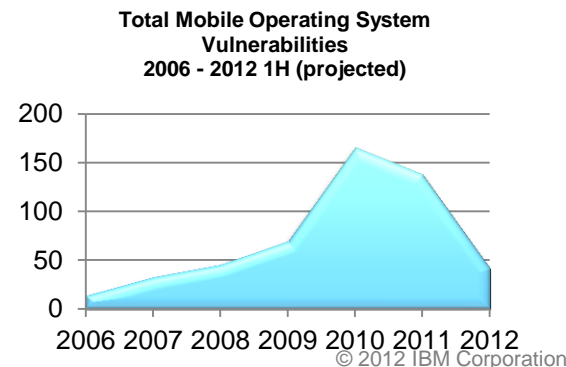
- A survey of consumer users found that one out of every three users has ever lost a mobile device.
- 2011 study - 36 percent of consumers in the United States have either lost their mobile phone or had it stolen. (Symantec)
- The major benefits of mobile devices (size and portability) unfortunately come with the big risk of losing sensitive data that has to be accepted but can be mitigated.
- Cell phone theft in New York City jumped from eight percent of robberies 10 years ago to more than 40 percent today (CBS News)

Communication

- SMS toll fraud continues as one of primary exploited areas
- Bluetooth is an exploited vector because a device in a discoverable mode can be easily discovered and lured to accept a malicious connection request.
- “Man in the middle” attacks have been demonstrated to be possible with several platforms using Wi-Fi links.
- Phishing or pharming attacks can leverage multiple channels: email, SMS, MSS, and voice

OS vulnerability based attacks

- Mobile OS vulnerabilities continue to be discovered at significant rates
- Always on and connected, mobile device is a prime target for hit-and-run network-based attacks and exploiting zero-day vulnerabilities.
- Published techniques to “jailbreak” or “root” mobile devices allow hackers to get administrative access, commonly within days of release



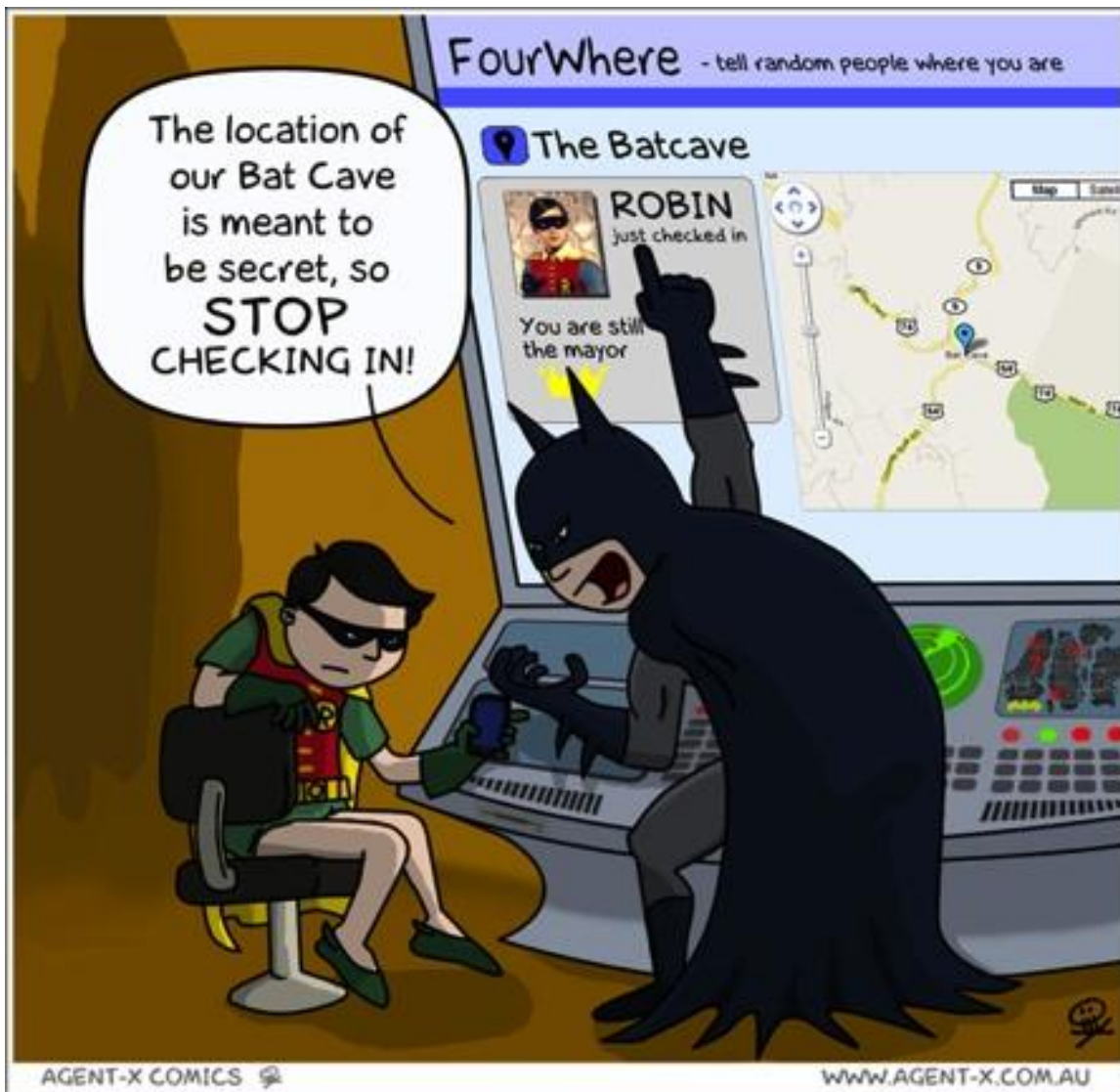
New Mobile threats

Which QR code is evil?



- QR Code contained a URL to download malware
- The malware sent SMS messages to a premium rate number (US \$6 per message)

<http://siliconangle.com/blog/2011/10/21/infected-qr-malware-surfaces-on-smartphones-apps/>



Social networks create an easy environment to share, but without editorial oversight this can lead to any number of problems.

Global Facebook Connections Map



Graph of 500M Facebook users' network connections, December 2010

Source: Paul Butler, Facebook: http://www.facebook.com/note.php?note_id=469716398919

Social Media in Your Organization

- Facebook is now the primary communication method for college students in the U.S. (Univ of Maryland Study)
- Social networking accounts for 22% of all time spent online in the U.S., and average workers spend 5.5 hours/month on social networking from the office (Nielson)
- Social networks are now the #1 activity on the Web
- Many employees use social media via personal devices at work without official permission
 - **1 in 3 Americans now own a smart phone, and 500M+ are expected to be sold in 2012**
 - **IDC: 95% of workers use technology they purchased themselves for work**
 - **Aberdeen: 72% of firms surveyed allow employees to use smartphones or tablets for work**



Social Media Risks Are Increasing

- Explosion of social networks encourages a high degree of communication and sharing, which can lead to increased risk
- Younger generations have a much lower expectation of (and respect for) privacy and security
- The massive amount of now public or open-source intelligence (OSINT) that is available for gathering has opened a new realm in information security and attacks.
- Potential security and privacy risks from employee misuse of social media
 - Exposure of confidential information
 - Use of inappropriate language / libelous speech
 - Misrepresentation of corporate positions
 - Potential legal liability and negative PR
 - Posting of confidential or embarrassing photos or videos
 - Increased risk of malware infections

In a recent survey, 63% of more than 4,000 respondents felt that social media represents increased security risks—yet only 29% reported that they had the necessary security controls to mitigate those risks.

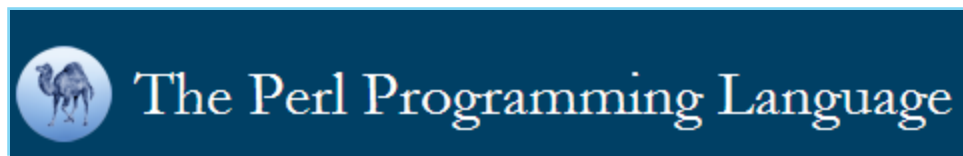
“Conventional marketing wisdom long held that a dissatisfied customer tells ten people. But...in the new age of social media, he or she has the tools to tell ten *million*.”

- Paul Gillin, *The New Influencers: A Marketer's Guide to Social Media*

Open Source – a foundation for the Web, but risk-laden!

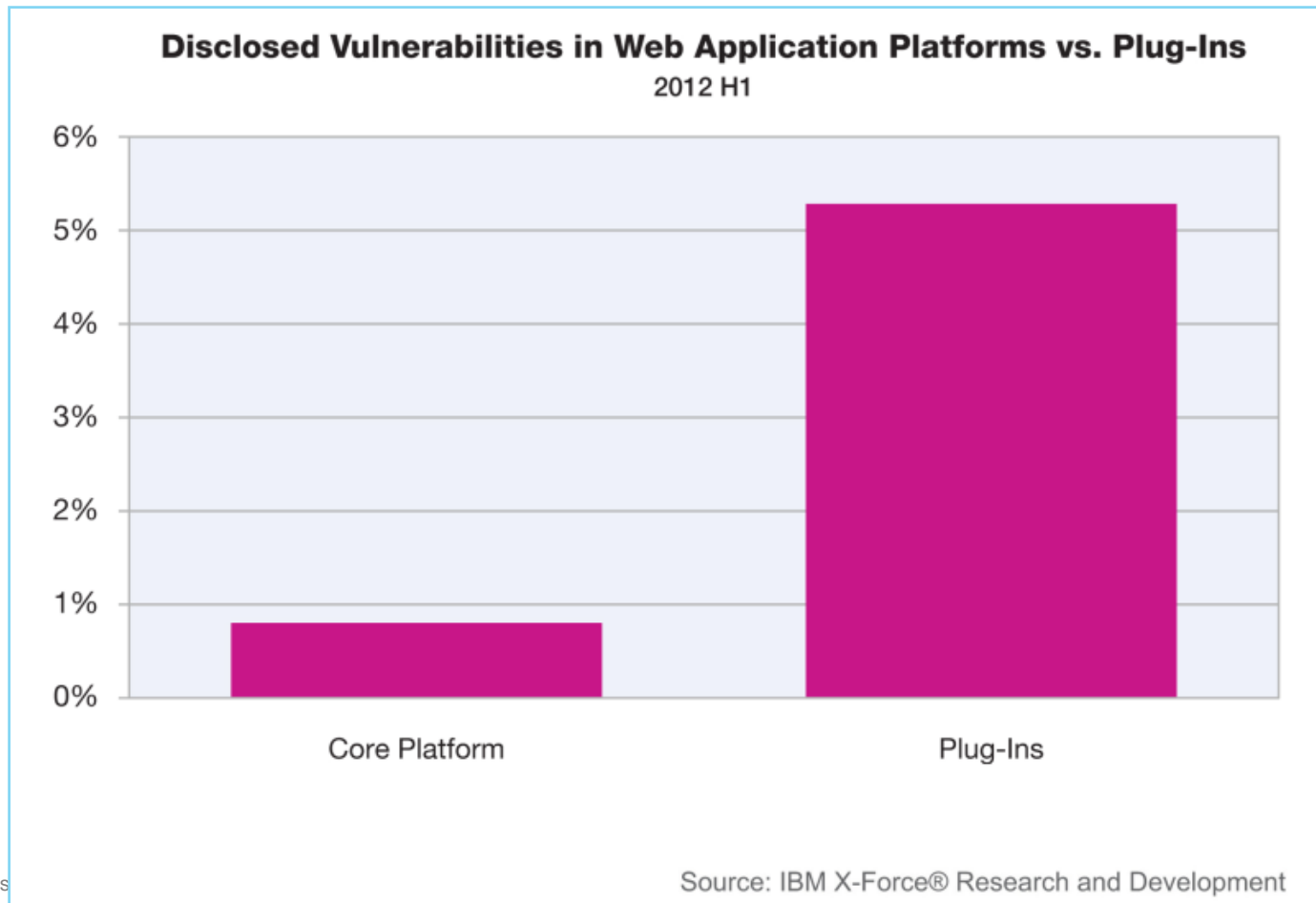


- Cost of Entry
 - Positive: allows many to innovate quickly and cheaply
 - Negative: allows attackers to deploy and use same tools
- Pervasiveness
 - Positive: Widely used around the world, can help to identify problems quickly
 - Negative: Increases appeal as a target, ensures vast base of potential victims
- Ease of Deployment (one click install)
 - Positive: does not require technical skills to deploy
 - Negative: More difficult to patch and maintain



Web Application vulnerabilities on public exploit websites

- Major web-based Content Management Systems (CMS) programs have become better at notifying the public when vulnerabilities are found in plug-ins written by third parties.
- Core issues are patched by the producing company that provides these systems at a much higher rate than the plug-ins written by third parties.





The Security Trends

Security teams must shift from a conventional “defense-in-depth” mindset and begin thinking like an attacker

Off-the-Shelf
tools and
techniques

Sophisticated

Audit, Patch & Block

***Think like a defender,
defense-in-depth mindset***

- ✓ Protect all assets
- ✓ Emphasize the perimeter
- ✓ Patch systems
- ✓ Use signature-based detection
- ✓ Scan endpoints for malware
- ✓ Read the latest news
- ✓ Collect logs
- ✓ Conduct manual interviews
- ✓ Shut down systems

Broad

Detect, Analyze & Remediate

***Think like an attacker,
counter intelligence mindset***

- ☐ Protect high value assets
- ☐ Emphasize the data
- ☐ Harden targets and weakest links
- ☐ Use anomaly-based detection
- ☐ Baseline system behavior
- ☐ Consume threat feeds
- ☐ Collect everything
- ☐ Automate correlation and analytics
- ☐ Gather and preserve evidence

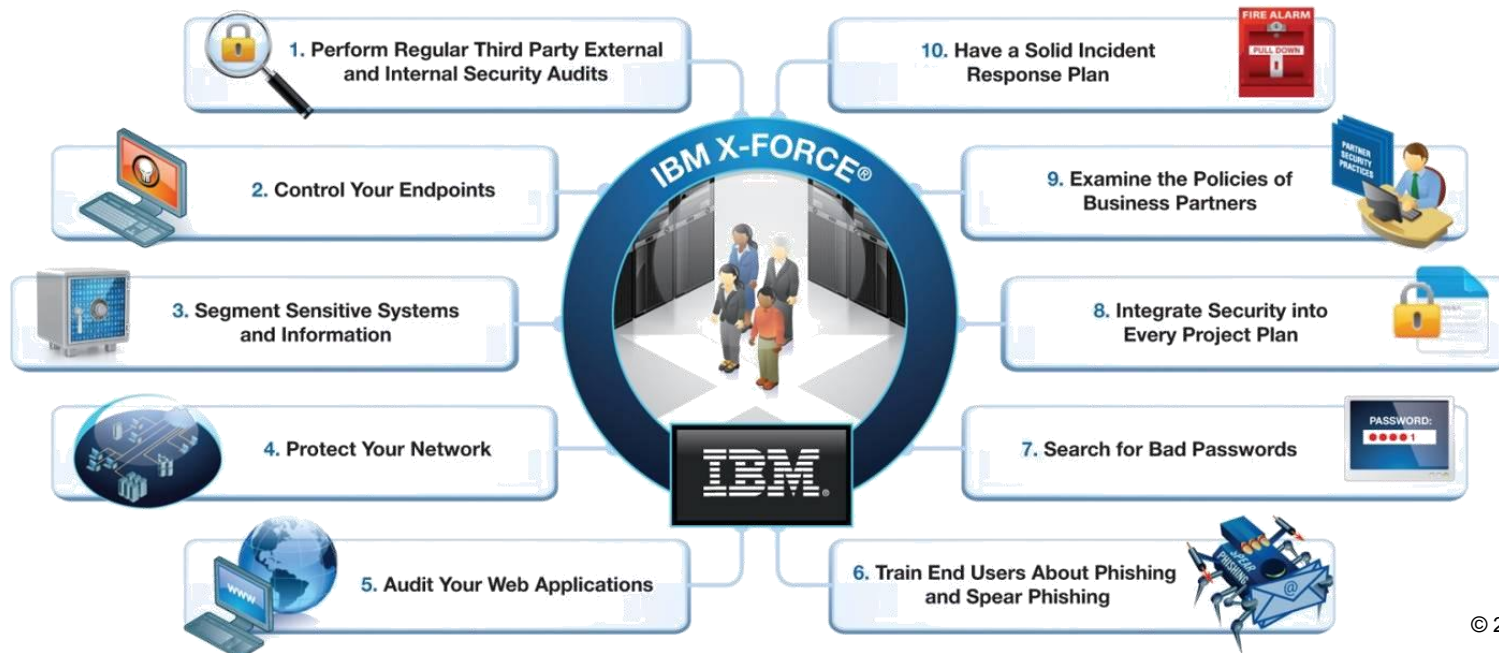
Targeted

Not a technical problem, but a business challenge

- Many of the recent breaches could have been prevented
- Significant effort is required to inventory, identify, and close every vulnerability
- Financial & operational resistance is always encountered, so how much of an investment is enough?

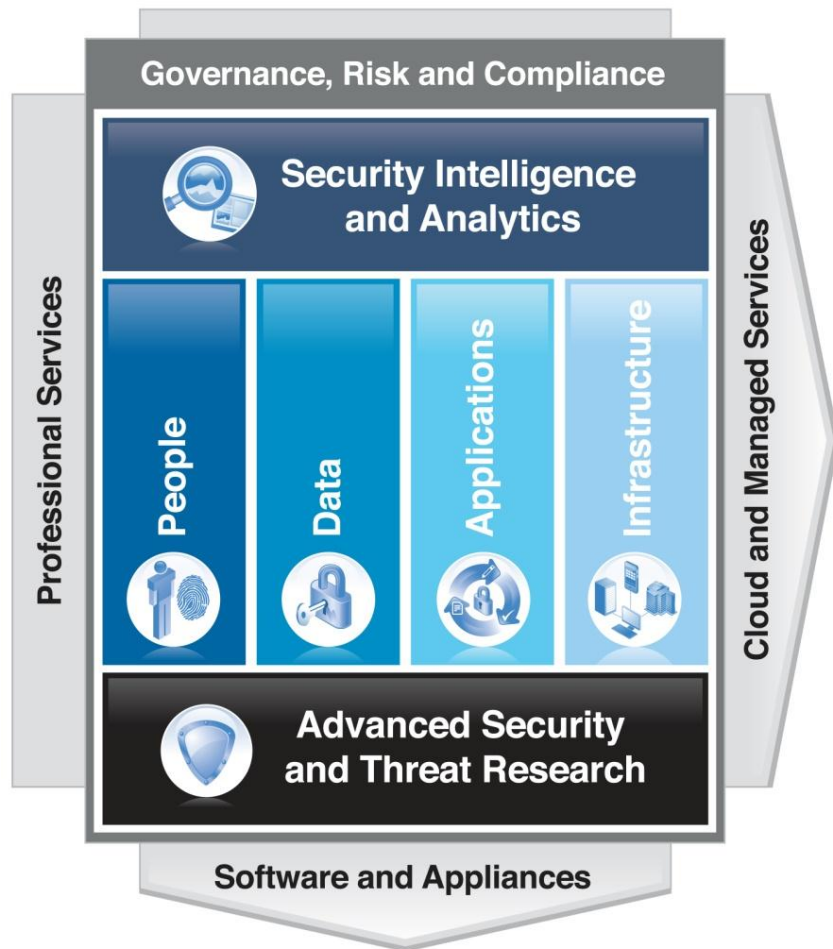
IF IBM X-FORCE® WAS RUNNING THE IT DEPARTMENT

Many readers have asked, if IBM X-Force were running the IT department and saw what happened this year, what would you do? Well, here are ten actions beyond the basics that X-Force would do if we ran the IT department.



IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

IBM Security Framework



IBM Security Systems

- IBM Security Framework built on the foundation of COBIT and ISO standards
- End-to-end coverage of the security domains
- Managed and Professional Services to help clients secure the enterprise

Get Engaged with IBM X-Force Research and Development



Follow us at @ibmsecurity
and @ibmxforce



Download X-Force
security trend & risk
reports

<http://www-935.ibm.com/services/us/iss/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



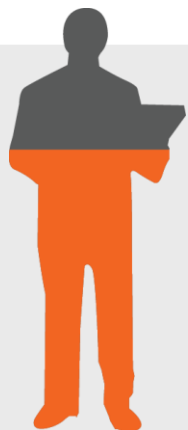
Subscribe to the security
channel for latest security
videos
www.youtube.com/ibmsecuritysolutions



Additional References

The Security Team

In IBM's 2012 Chief Information Security Officer Study, security leaders described the changing landscape...



Nearly two-thirds say **senior executives** are paying **more attention** to security issues.



Two-thirds expect to **spend more** on security over the next two years.



External threats are rated as a **bigger challenge** than internal threats, new technology or compliance.

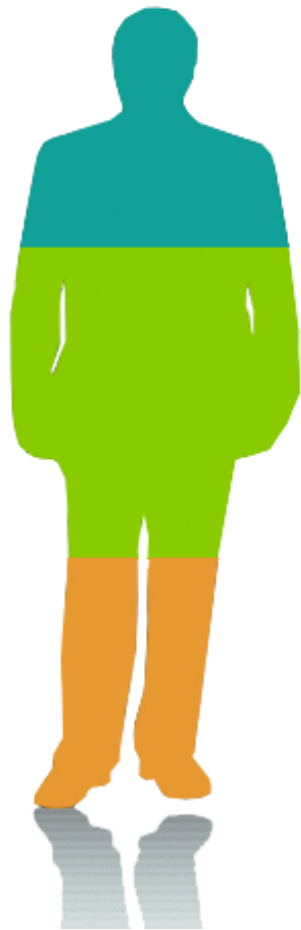


More than one-half say **mobile security** is their greatest near-term **technology concern**.

Source: IBM 2012 CISO Assessment

http://www.ibm.com/smarterplanet/us/en/business_resilience_management/article/security_essentials.html

...And the changing role of the CISO



Influencers

- Confident, prepared
- Strategic influence

Influencers

- Less confident
- Strategic priorities, but lack structural elements

Responders

- Least confident
- Focus on protection and compliance

How they differ

have a dedicated CISO



have a security/risk committee



have information security as a board topic



use a standard set of security metrics to track their progress



focused on improving enterprise communication/collaboration



focused on providing education and awareness



IBM Cyber Security Innovation program




23% of organizations have a “problematic shortage” of IT security skills

Objectives

- Build curriculum, skills, and expertise in Cyber Security Services and Security Engineering
- Partner with the academic community, worldwide, while amplifying work done by top Faculty members
- Dramatically improve skills in Asia Pacific, Central and Eastern Europe, Latin America, Middle East and Africa

150+ Academic institutions have been identified – including UNCC

The IBM Academic Initiative Security Portal



Country/region [select]

Search

[Home](#)
[Solutions ▾](#)
[Services ▾](#)
[Products ▾](#)
[Support & downloads ▾](#)
[My IBM ▾](#)

IBM Academic Initiative


- Membership
- Teaching topics
- Software & hardware
- Courseware
- Training & certification
- Community
- Support
- Technical library

[IBM Academic Initiative > Teaching topics >](#)

Information assurance and security

IBM resources to enhance your curriculum

[↓ Learn about security](#)
[↓ Teach your students](#)
[↓ Connect with others](#)



Security has ascended in importance across businesses of all sizes, whether it's the CMO evaluating the potential risk to the brand, the CFO understanding the financial implications of adverse events, or the COO assessing the impact of IT systems disruptions on ongoing operations.

Learn about security

Developing security intelligence skills — the ability to proactively predict, identify and react to potential threats — will take on a new priority in the digital age. Read these documents to understand the important trends and opportunities emerging in the information security profession worldwide.

- [2011 ISC2 Global Information Security Workforce Study](#) conducted by Frost & Sullivan, reports a clear gap in skills needed to protect organizations in the near future.
- [Managing threats in the digital age](#) explains the growing importance of security intelligence skills.
- [Clearing the clouds: Shining a light on successful Enterprise Risk Management](#) discusses the Enterprise Risk Management as a hot new career.
- [Combating risk with predictive intelligence](#) shows how leading risk management practices are proactively mitigating and managing complexity-fraught risks.

Teach your students about security

Membership

- Overview
- Join now
- Renew

University partners

Fraunhofer Institute for Secure Information Technology (FIH SIT) is a research partner with IBM Böblingen Labs

- [FIH SIT \(English\)](#)
- [FIH SIT \(German\)](#)

Technical University of Darmstadt (TUD) hosts the European Center for Security and Privacy by Design

- [Master's program in IT Security](#)

Related links

- [IBM Student Portal](#)
- [IBM developerWorks](#)
- [alphaWorks](#) (emerging technologies)

Academic Initiative regional sites

- [Brazil](#)
- [China](#)
- [Germany](#)
- [India](#)
- [Italy](#)
- [Japan](#)
- [Russia](#)

IBM Relaunches CIO / CISO Institute for Advanced Security



IBM Institute for Advanced Security
Where global security leaders go to share intelligence and collaborate

Home | Expert Blog | Departments | Topics | Global Branches | Resource Library | Events | Join

September 17, 2012: Building a Secure Supply Chain

VIEWPOINT
Supply Chain Security: Becoming a Trustworthy Provider
By Andras Szakal
Cybersecurity considerations must be addressed in a sustainable way from the get-go, by design, and across the whole ecosystem. [Read More](#)

ESSENTIALS FOR CIOs/CISOs
Securing the Extended Enterprise
Enterprises must take vigorous steps to keep their entire information ecosystem secure, including vendors, suppliers, contractors, acquisitions and partners. The challenge is to implement policies and best practices governing your data, no matter where it goes. [Read More in the Whitepaper](#)

AT A GLANCE
Extending the security perimeter
1. Build security into every relationship—from the start.
2. Develop tight procedures for M&A—from due diligence through integration
3. Extend your focus to your partner's suppliers—both large and small
4. Assume that nothing is ever settled

TOP OF MIND
Link-quisitiveness: Lessons from History on Secure Supply Chains
By Jack Danahy
A few years ago, while researching some new historical references to help people better understand their own responsibilities in a changing computing environment, I came up with examples from other industries where lessons can be learned. [Read More](#)

ASK JACK
Have a question for Jack Danahy, Director of Advanced Security at IBM? [Blog and](#)

CONNECTIONS
blogtalkradio Podcast: Be Prepared - the Latest Research from IBM X-Force with details from the 2012 Mid Year Trend and Risk Report, hosted by Caleb Barlow. September 20th at 10am EST. [Register Here](#)
Webcasts SCMag UK Virtual Event: "Avoiding the Front Page: Strategies to Stay Out of the Headlines" - with Chris Poulin, Security Systems Strategist, IBM Security Division; and Bola Rotibi, Founding Member (ISC)2 security board. September 26, 2012, 10-11 AM (ET). [Register Now](#)
User Group Meeting

A new focus on educating and enabling CISO's and security-minded CIO's

- ▶ 907 members
- ▶ 267 pieces of content
- ▶ Weekly themes on Security topics
- ▶ Webcasts, podcasts, blogs, whitepapers, and events
- ▶ Recruiting external content from non-IBM SME's

<http://instituteforadvancedsecurity.com/>

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.