



IBM Security

Intelligence. Integration. Expertise.

Steve Robinson, VP Development, Strategy, and Product Management,
IBM Security Systems Division

Denis Kennelly, VP Security Development, IBM Security Systems Division

Pulse2012

Meet the Experts. Optimise your infrastructure.

May 31 – June 1

Sheraton on the Park Hotel, Sydney

Please note:

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

The Journey Toward a Smarter Planet Continues

Smart Supply Chains



Smart Countries



Smart Retail



Smart Water Management



Smart Weather



Smart Energy Grids



INSTRUMENTED



INTERCONNECTED



INTELLIGENT

Smart Oil Field Technologies



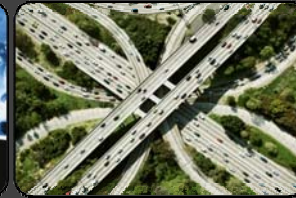
Smart Regions



Smart Healthcare



Smart Traffic Systems



Smart Cities



Smart Food Systems





ATTACK SOPHISTICATION

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





CLOUD

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





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



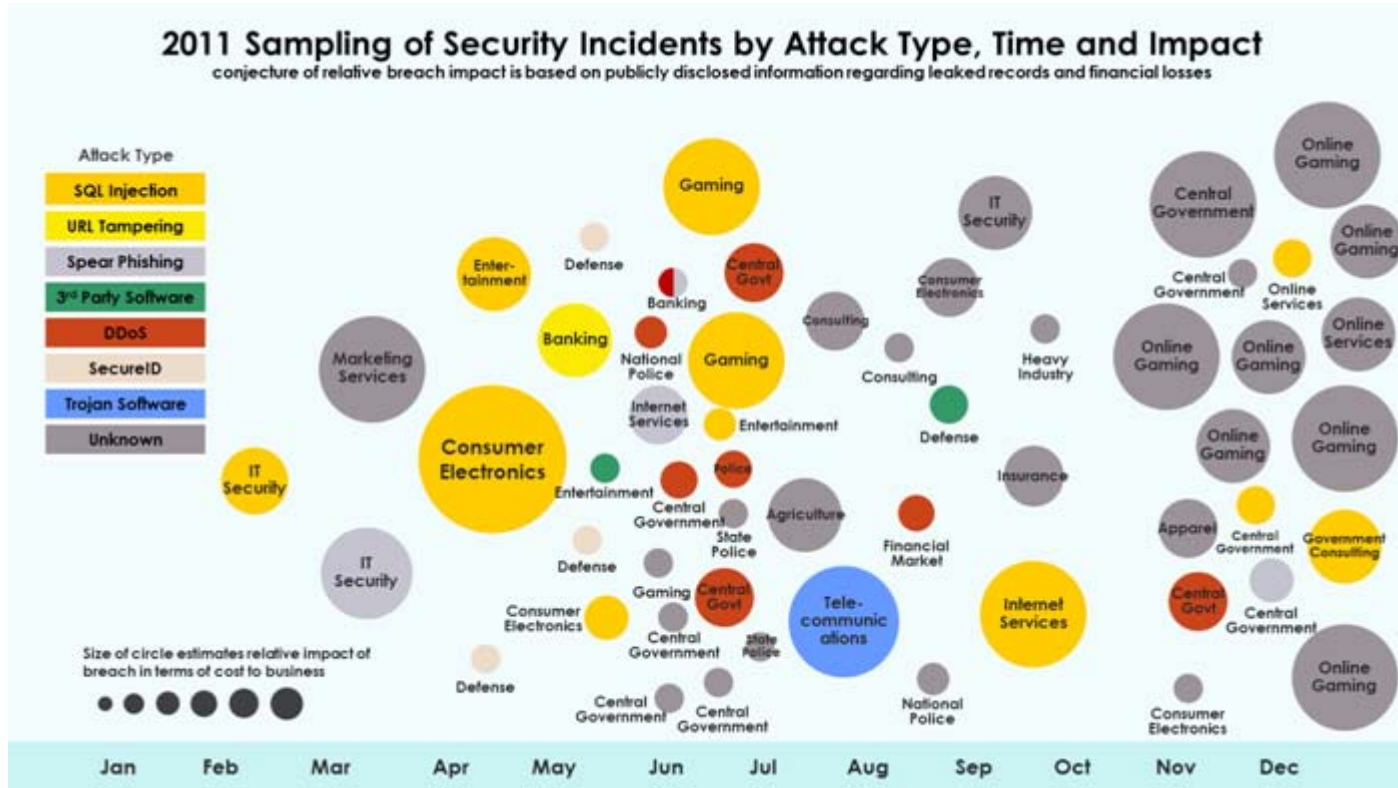
DATA EXPLOSION

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



Security Threats Are Accelerating

Targeted attacks shake businesses and governments



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

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 Hactivism

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

Audit Risk

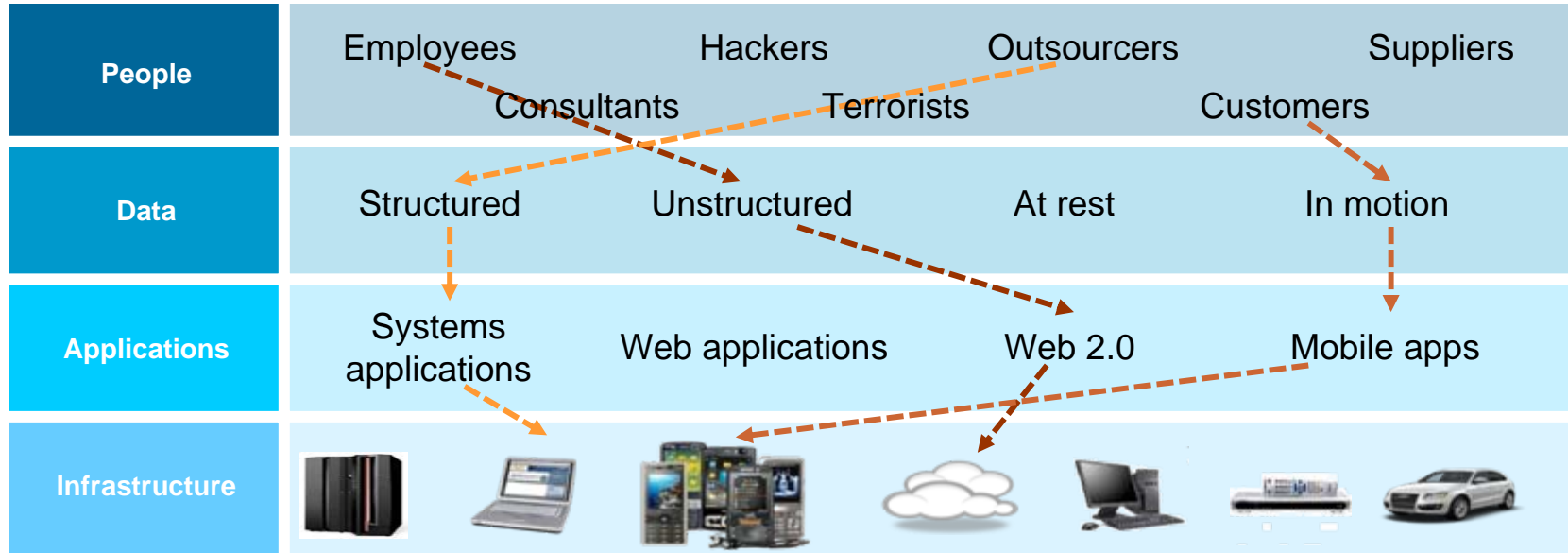
Zurich Insurance PLC fined £2.275M (\$3.8M) for the loss and exposure of 46K customer records

IT Security Is a Board Room Discussion



IBM's Security Strategy

Solving a Security Issue Is a Complex, Four-dimensional Puzzle

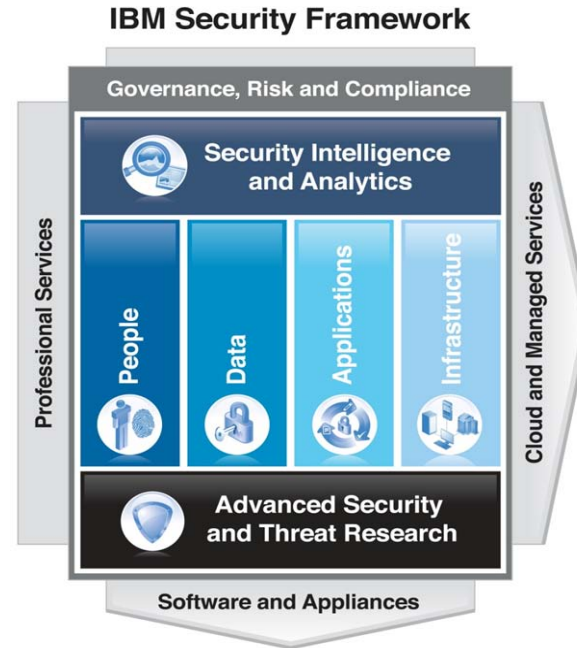


Attempting to protect the perimeter is not enough – siloed point products cannot adequately secure the enterprise

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

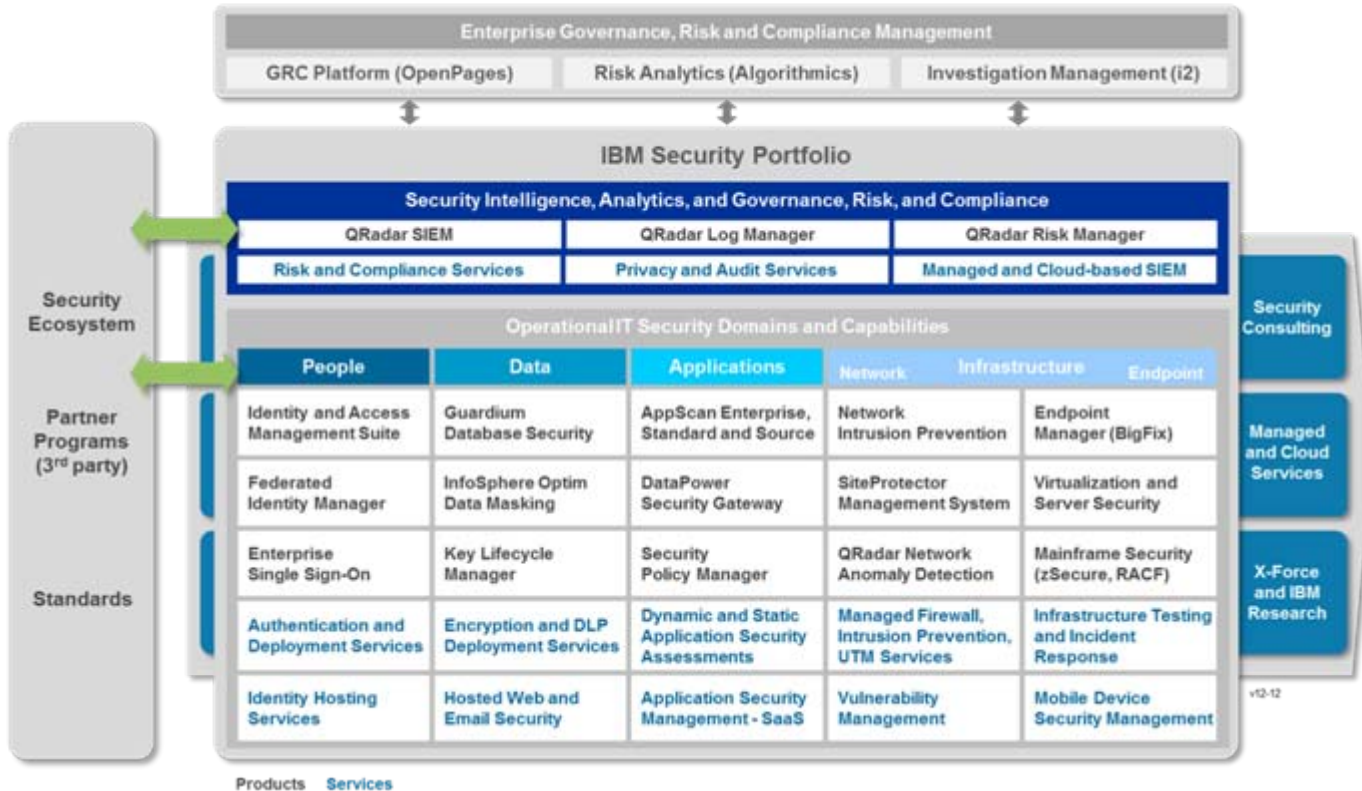
IBM Security Systems

- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- One of the largest vulnerability databases



Intelligence • Integration • Expertise

Intelligence: A comprehensive portfolio of products and services across security domains



Integration: Increased security, collapsed silos, reduced complexity

Integrated Intelligence.



- Consolidate and correlate siloed information
- Detect, notify and respond to threats
- Automate compliance tasks and assess risks

Integrated Research.



- Detect the latest exploits, vulnerabilities, and malware
- Automatically update SW
- Add security intelligence to non-intelligent systems





Integrated Protection.

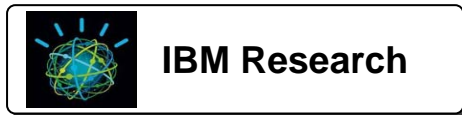


- Block specific vulnerabilities using scan results
- Converge access mgmt with web service gateways
- Link identity information with database security

Expertise: Global coverage and security awareness



-  9 Security Operations Centers
-  9 Security Research Centers
-  14 Security Solution Development Centers
-  3 Institute for Advanced Security Branches



14B analyzed Web pages & images
 40M spam & phishing attacks
 54K documented vulnerabilities
 Billions of intrusion attempts daily
 Millions of unique malware samples



World Wide Managed Security Services Coverage

- 20K+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)



IBM Is Helping Clients Tackle Complex Security Challenges

Who Is Attacking Our Networks?

Attacker Types and Techniques 2011 H1

Off-the-Shelf tools and techniques

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS



Sophisticated

- Cyberwar

Broad

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)



- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

Targeted

Source: IBM X-Force® Research and Development

Advanced Persistent Threat (APT) Is Different

1 Advanced

- Exploiting unreported vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, researched attacks using multiple vectors

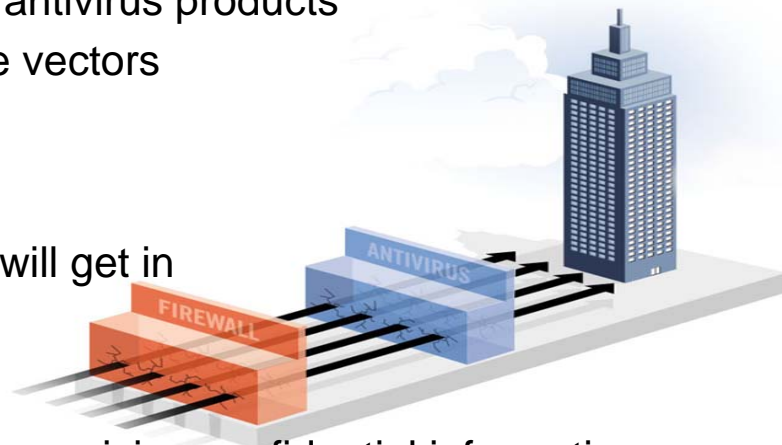
2 Persistent

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in

3 Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are “out to get you”

4 Responding is different too – **Watch, Wait, Plan** ... and call the FBI



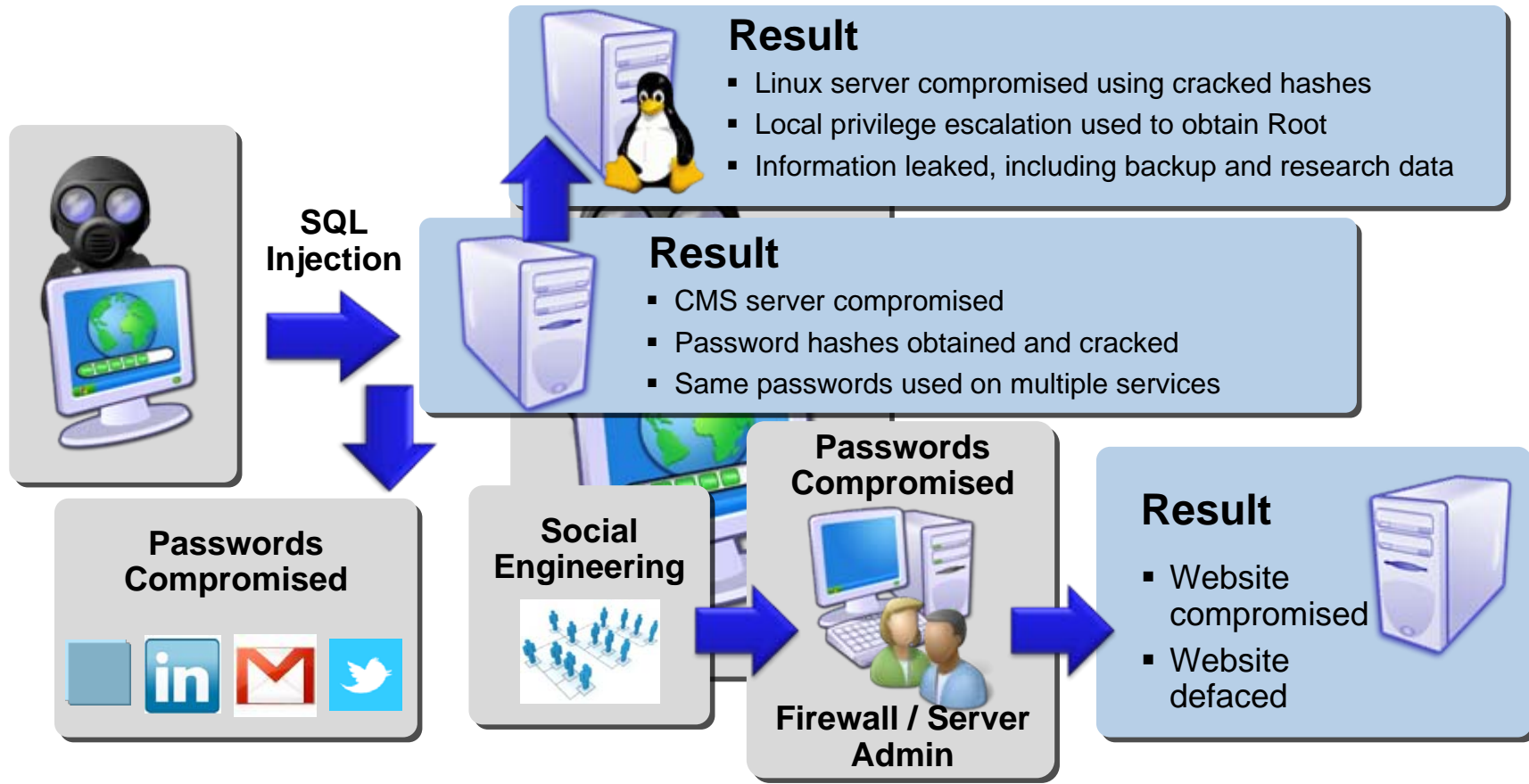
Internet Intelligence Collection

- Scan the corporate website, Google, and Google News
 - Who works there? What are their titles?
- Search for LinkedIn, Facebook, and Twitter Profiles
 - Who do these people work with?
 - Fill in blanks in the org chart
- Who works with the information we want to target?
 - What is their reporting structure?
 - Who are their friends?
 - What are they interested in?
 - What is their email address?



Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



SQL
Injection



Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



**Poor password
hashing**



Well Known, Off the Shelf Attack Techniques Are All That It Takes

As Anatomy of an APT – Scenario 1

Privilege escalation

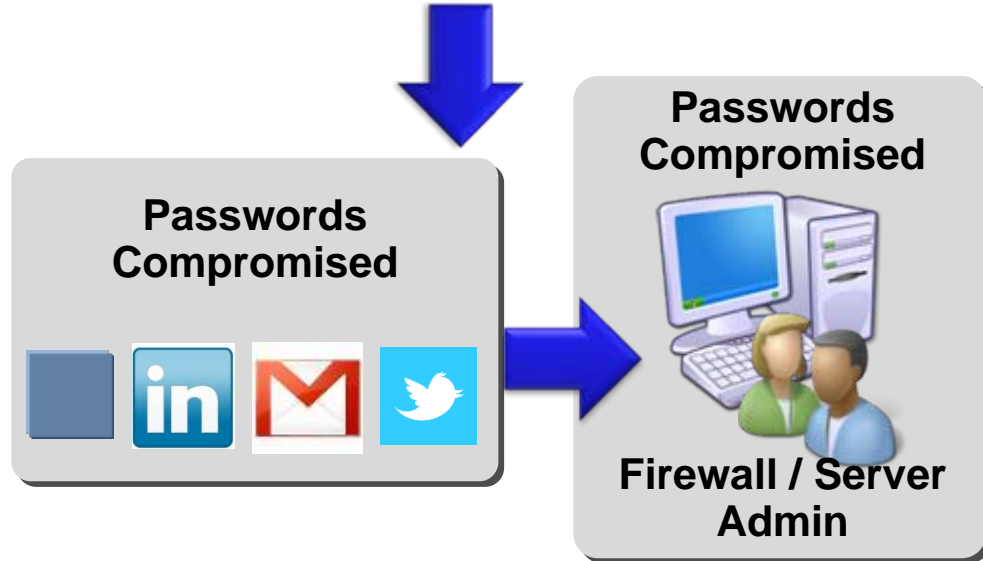
SSH



Patch management to fix privilege escalation

Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



Well Known, Off the Shelf Attack Techniques Are All That It Takes

As Anatomy of an APT – Scenario 1



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*

3rd Party
Software Update Server
Compromised

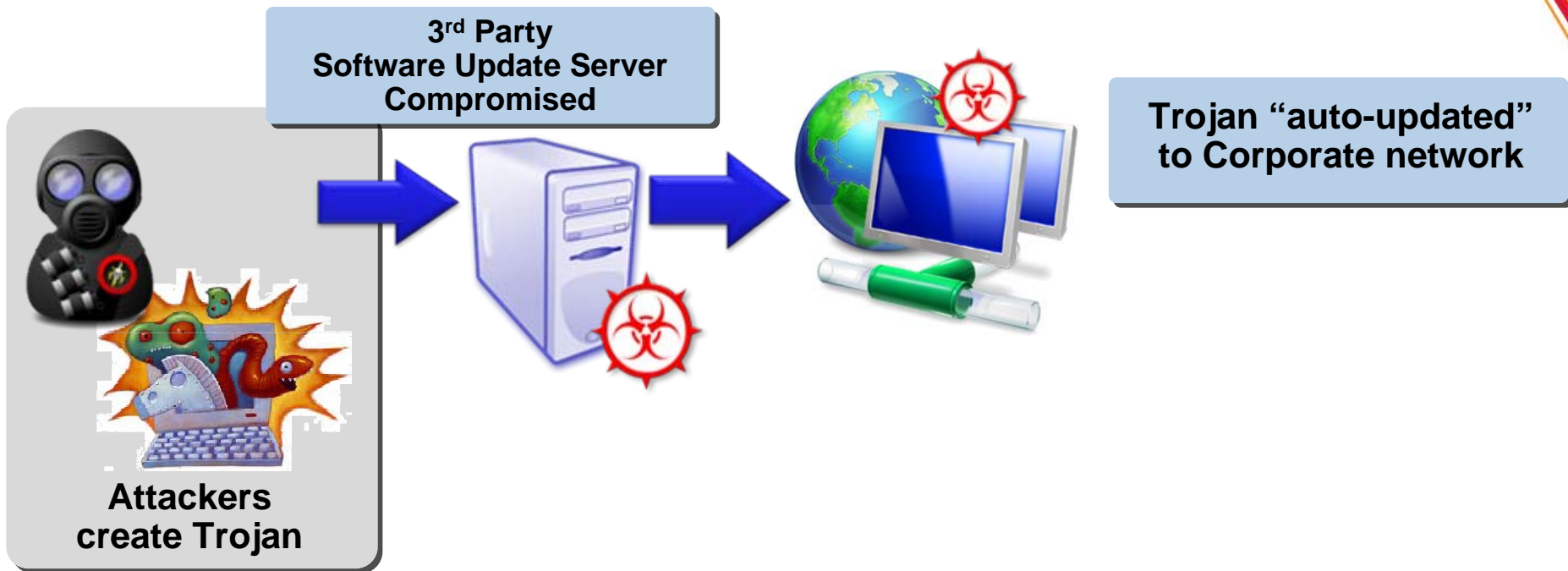


Attackers
create Trojan

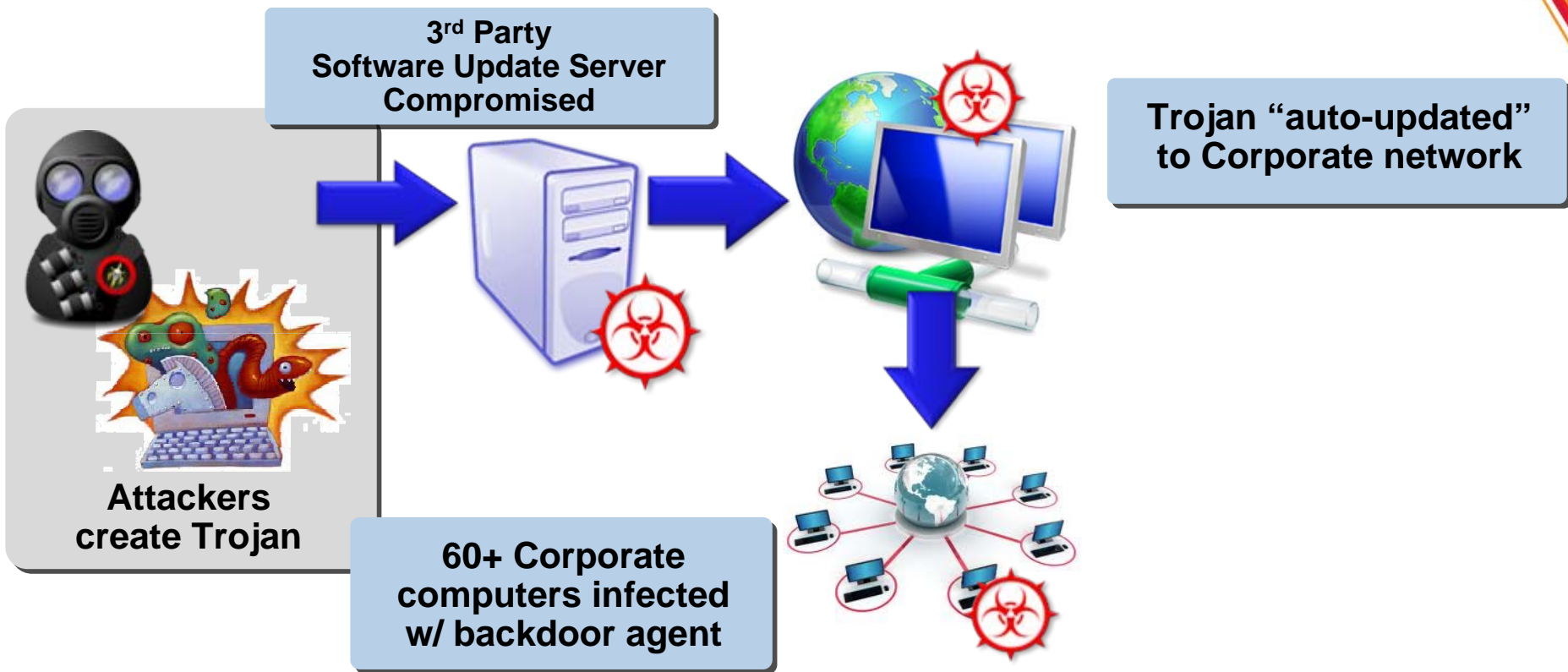


Attackers
create Trojan

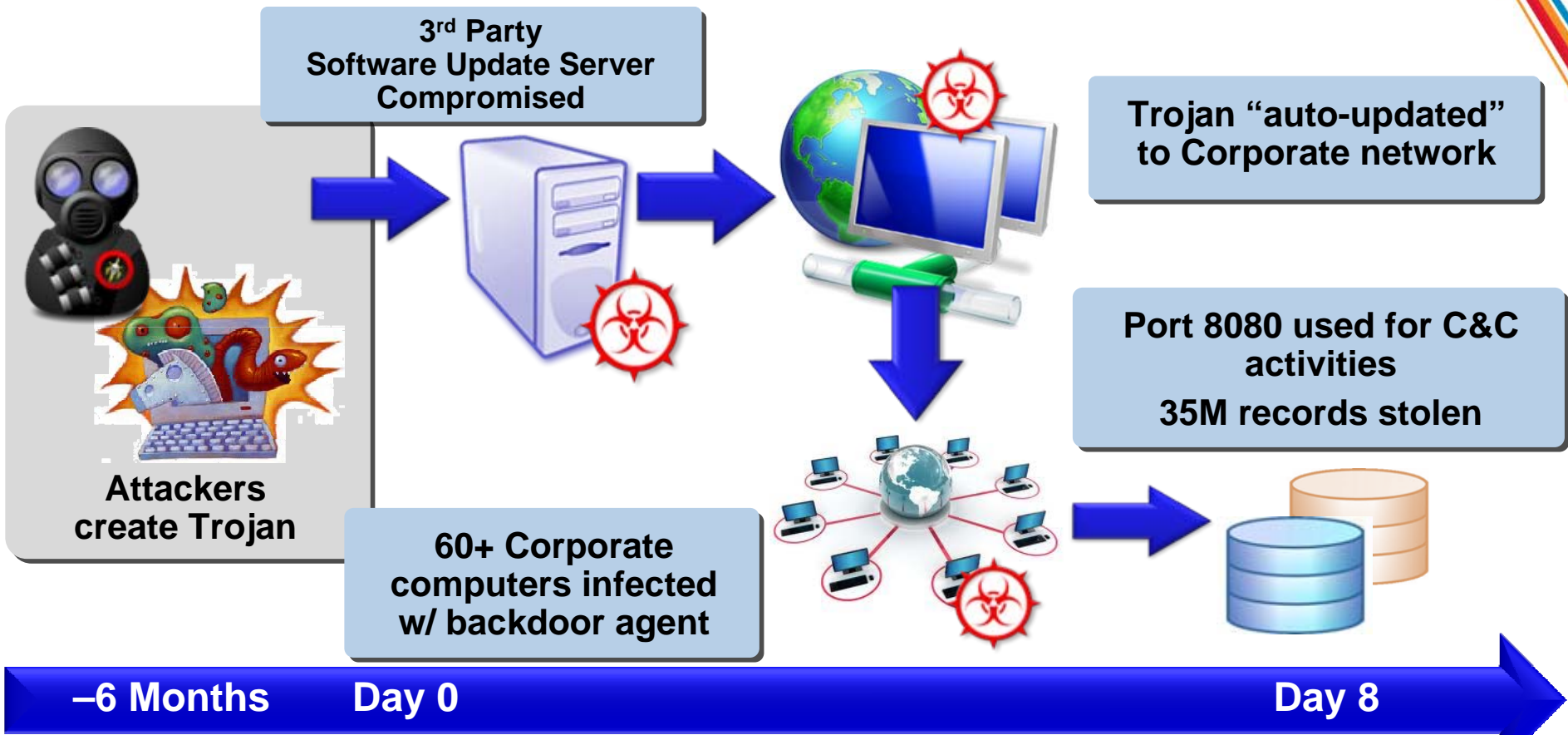
They Will Get In...Then What? *Anatomy of an APT – Scenario 2*



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*

3rd Party
Software Update Server
Compromised



Attackers
create Trojan

**Business
Partner
Security**



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*

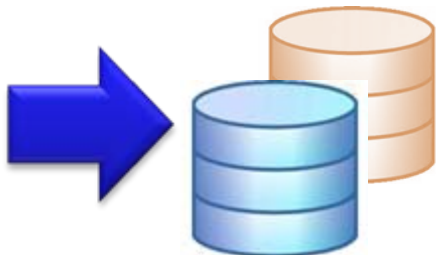


**60+ Corporate
computers infected w/
backdoor agent**



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*

Port 8080 used for C&C activities
35M records stolen



They Will Get In...Then What? *Anatomy of an APT – Scenario 2*





The Path to Security Intelligence

IBM is investing in solutions to key trends driving the next wave of security innovation

Advanced Threats



Advanced Persistent Threats.
Designer Malware.
Stealth Bots. Zero-days.
Targeted Attacks.

Cloud Computing



Mobile Computing



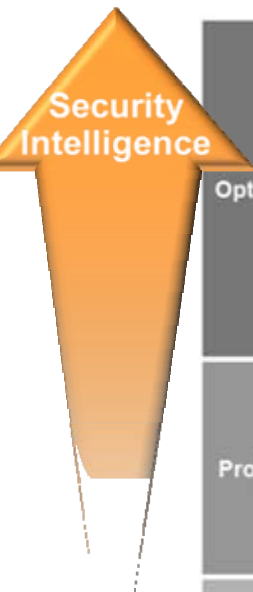
Enterprise Customers



Regulation and Compliance



Security Intelligence is enabling progress to optimized security



	Security Intelligence: Information and event management Advanced correlation and deep analytics External threat research			
Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure application engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Security rich systems
Proficient	User provisioning Access management Strong authentication	Database vulnerability scanning Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset management Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus
	People	Data	Applications	Infrastructure



Helping define the new role of the information security leader and tracking security trends



<http://instituteforadvancedsecurity.com/content-library/m/files/97.aspx>



https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report

Acknowledgements, disclaimers and trademarks

© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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 this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation 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. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml



Trademarks and disclaimers

© Copyright IBM Australia Limited 2012 ABN 79 000 024 733 © Copyright IBM Corporation 2012 All Rights Reserved. TRADEMARKS: IBM, the IBM logos, ibm.com, Smarter Planet and the planet icon are trademarks of IBM Corp registered in many jurisdictions worldwide. Other company, product and services marks may be trademarks or services marks of others. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

