IBM Business Connect

Business Without Limits.

July 18 | Sandton Convention Centre, Johannesburg

IBM Working Smarter For The Future

Greg Sinclair

18 July 2013

https://www.facebook.com/IBMSouthAfrica/events

#IBMBC2013

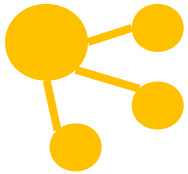
Understanding Your Organizational Security Posture

Security Intelligence

Innovative technology changes everything

1 trillion connected objects

1 billion mobile workers

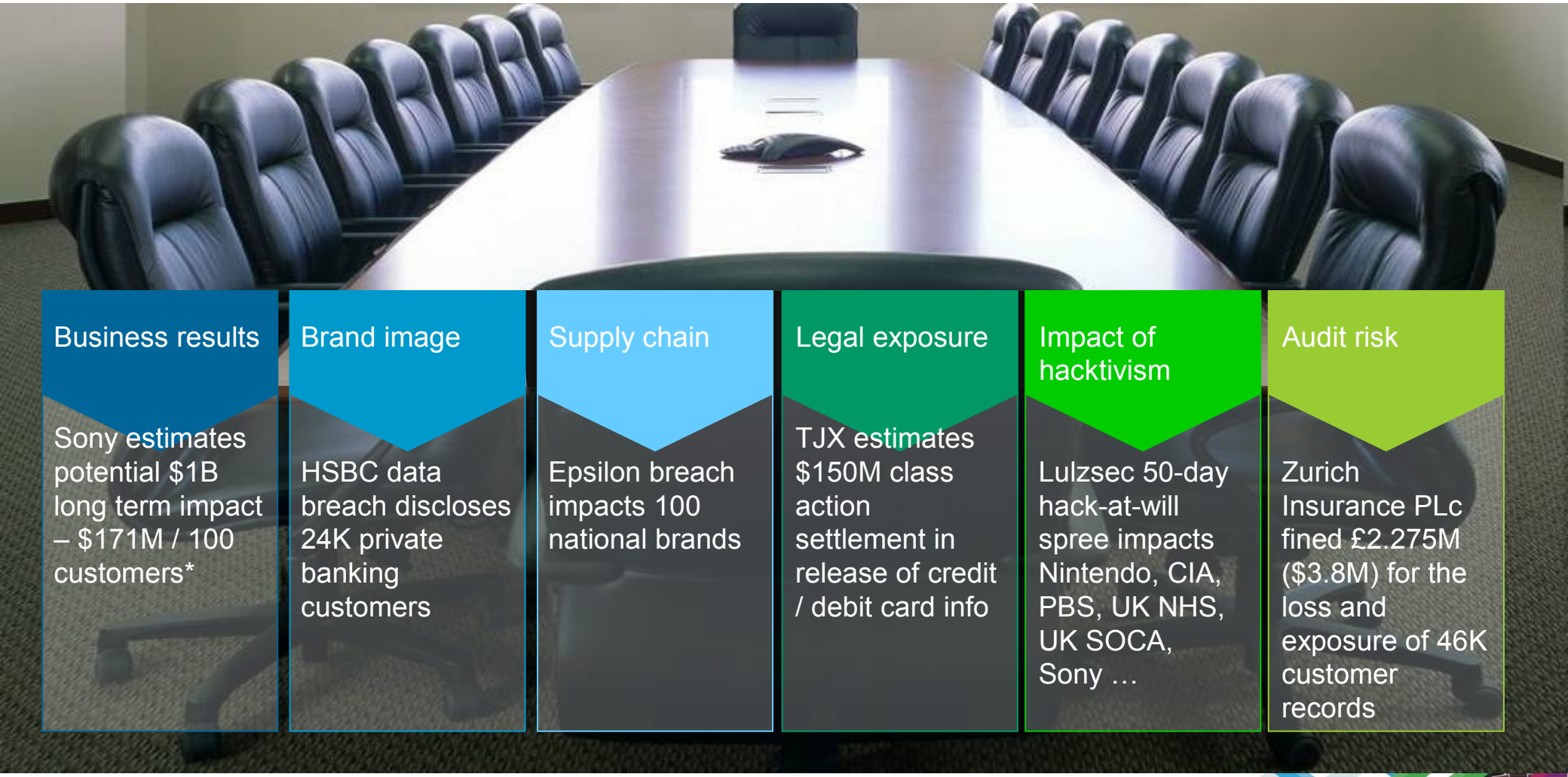


Social business

Bring your own IT

Cloud and virtualization

Propelling IT Security to a board room discussion



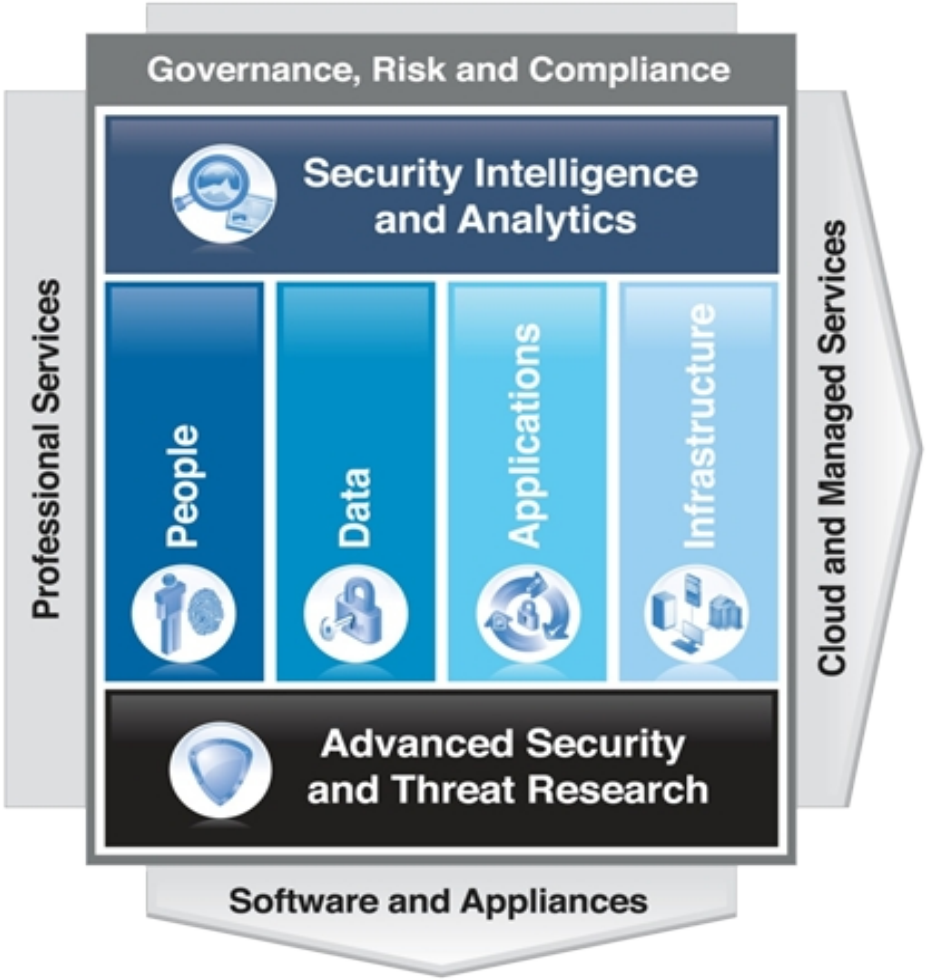
Business results	Brand image	Supply chain	Legal exposure	Impact of hacktivism	Audit risk
Sony estimates potential $1B long term impact – $171M / 100 customers*	HSBC data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement in release of credit / debit card info	Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …	Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

IBM delivers solutions across a security framework

Intelligence

Integration

Expertise



What is Security Intelligence?

Security Intelligence

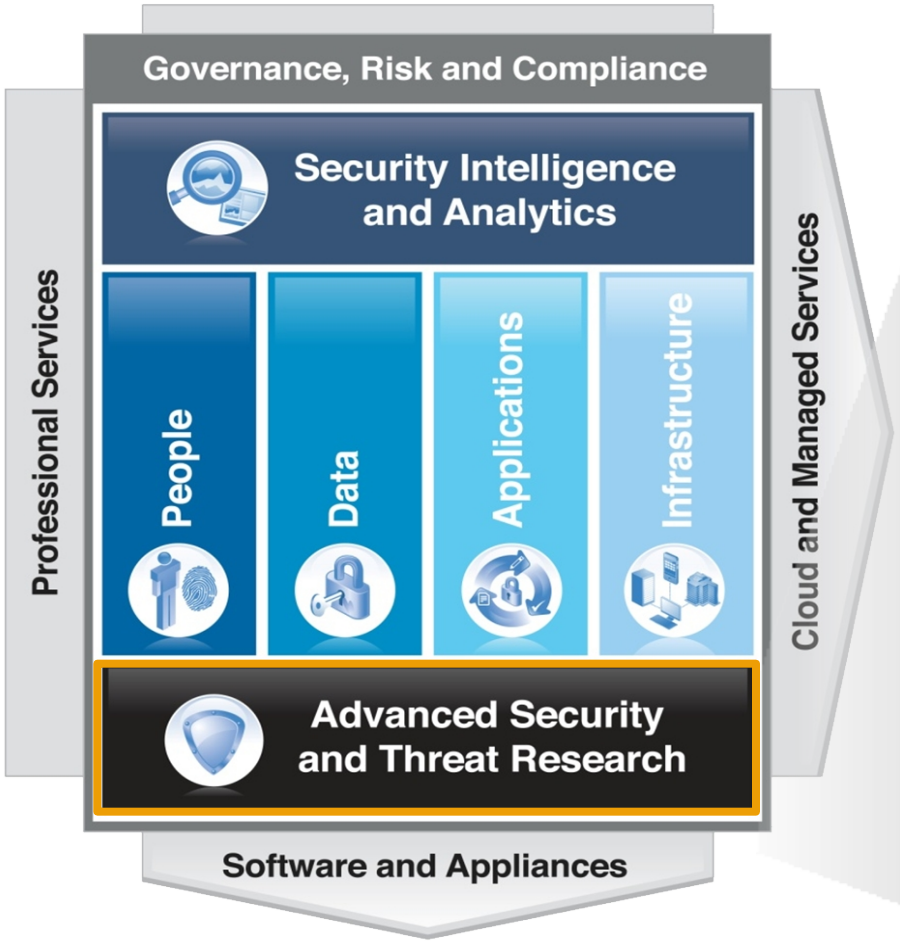
--noun

1. the real-time collection, normalization and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

IBM X-Force 2012 Full-Year Trend and Risk Report

X-Force is the foundation for advanced security and threat research across the IBM Security Framework



X-FORCE

The mission of X-Force is to:

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public

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

X-FORCE

IBM Research

Depth

17B analyzed web pages & images

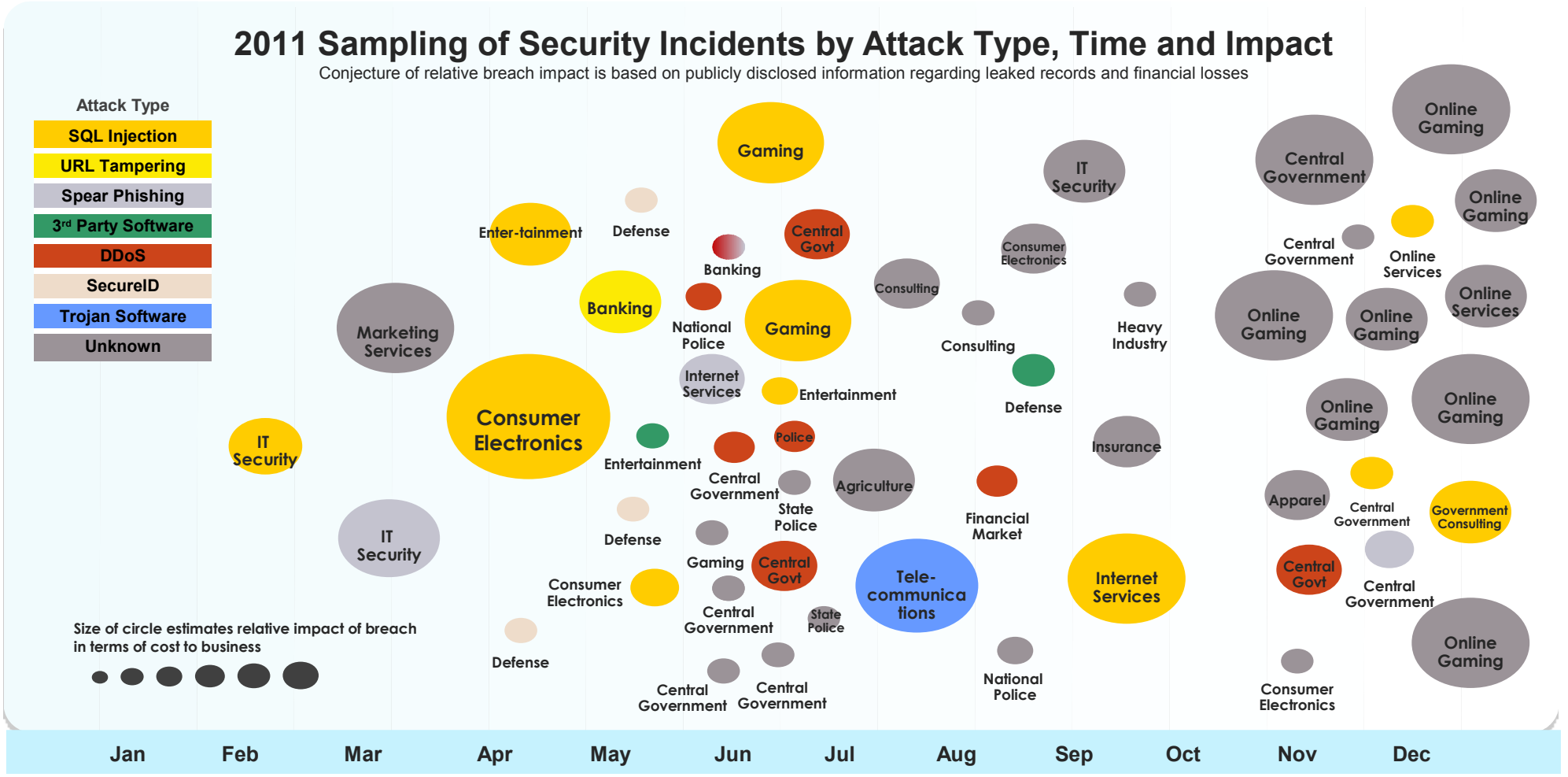
40M spam & phishing attacks

80K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

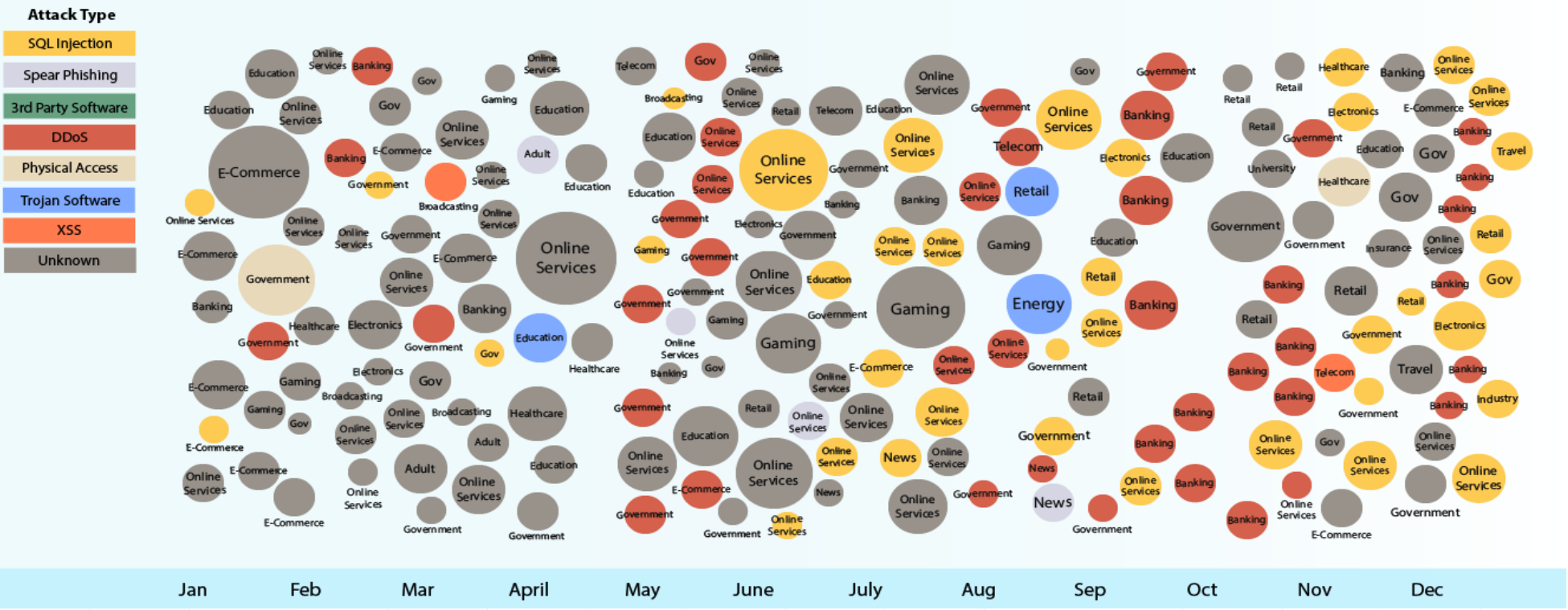
2011: “The year of the targeted attack”



2012: The explosion of breaches continues!

2012 Sampling of Security Incidents by Attack Type, Time and Impact

Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



Size of circle estimates relative impact of incident in terms of cost to business

Source: IBM X-Force® Research 2012 Trend and Risk Report

What are we seeing? Key Findings from the 2012 Trend Report

Threats and Activity

- 40% increase in breach events for 2012
- Sophistication is not always about technology
- SQL Injection, DDoS, Phishing activity increased from 2011
- Java means to infect as many systems as possible

Operational Security

- Software vulnerability disclosures up in 2012
- Web application vulnerabilities surge upward
- XSS vulnerabilities highest ever seen at 53%
- Content Management Systems plug-ins provide soft target

Emerging Trends

- Social Media leveraged for enhanced spear-phishing techniques and intelligence gathering
- Mobile Security should be more secure than traditional user computing devices by 2014

Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports
http://www-03.ibm.com/security/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or X-Force Security Insights blog at http://www.ibm.com/blogs/xforce

A Holistic Approach to Advanced Persistent Threats

How IBM is Helping Clients

S. Rohit
rohits@sg.ibm.com

Agenda

The Challenge of Advanced Persistent Threats

IBM's Comprehensive Security Portfolio

IBM's Approach

137,400,000

…Number of cyber-attacks witnessed by IBM in 2012

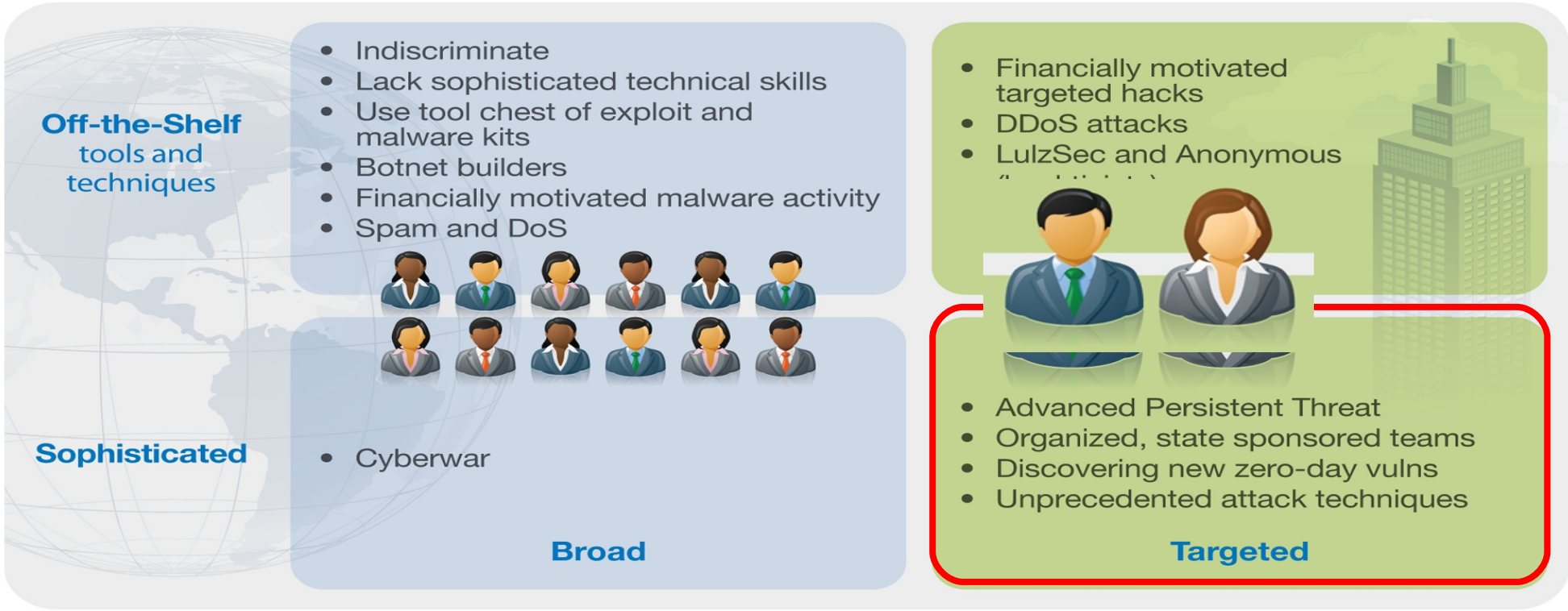
Most Attacked Industries

Industry	Average weekly attacks
Health and Social Services	10.1 million
Transportation	9.8 million
Hospitality	5.5 million
Finance and Insurance	3.6 million
Manufacturing	2.6 million

1.07

Incidents per
one million attacks[1]

Attackers are using sophisticated techniques to bypass defenses



"Advanced Persistent Threat" is the approach often used by State-Sponsored Entities

Source: IBM X-Force Research and Development

What's different about Advanced Persistent Threats?

Advanced

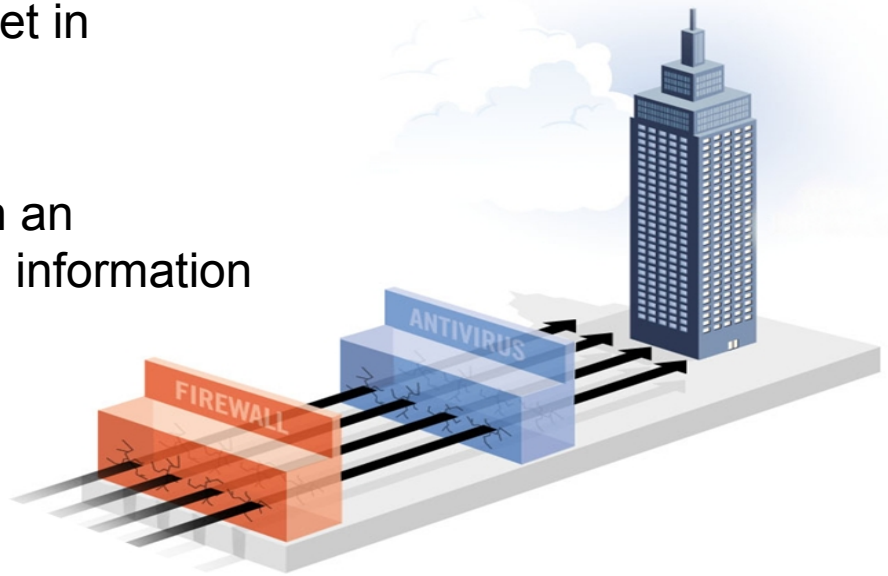
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

Persistent

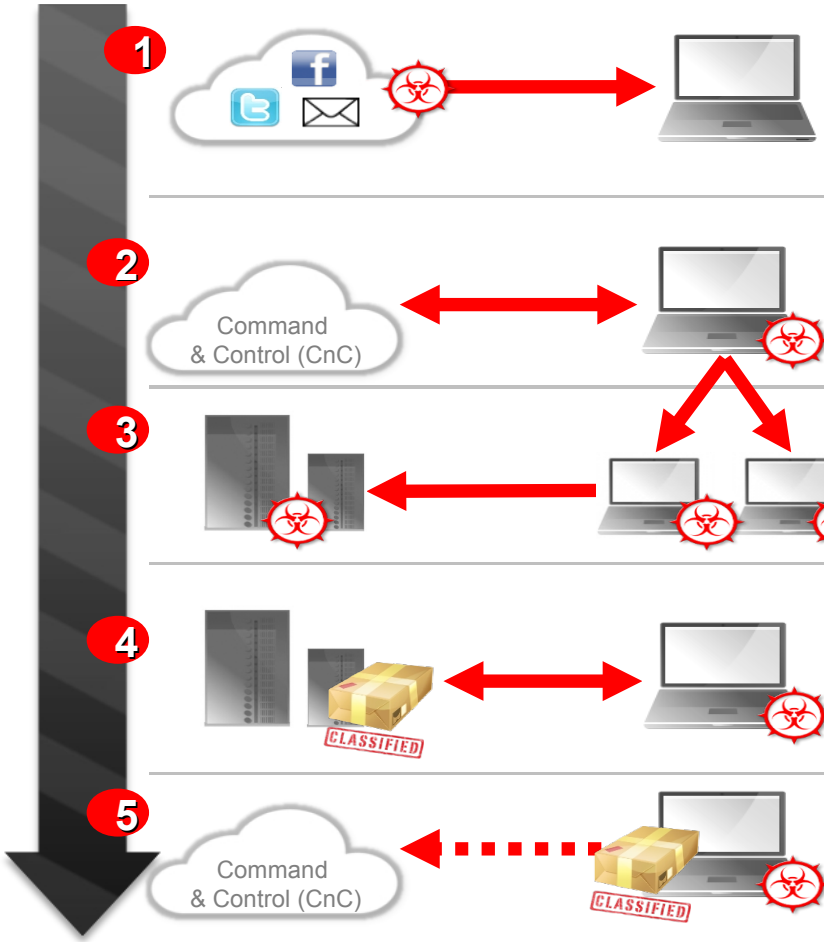
- Attacks last for months or years (average: 1 year; longest: 4.8 years)[1]
- Attackers are dedicated to the target – they will get in

Threat

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



Attackers follow a 5-Stage attack chain



Break-in

Spear phishing and remote exploits to gain access

Latch-on

Malware and backdoors installed to establish a foothold

Expand

Reconnaissance and lateral movement to increase access and maintain a presence

Gather

Acquisition and aggregation of confidential data

Exfiltrate

Data exfiltration to external networks

IBM's unique approach to security

- Leader in security software and services – recognized by Gartner, Forrester and IDC
- Solutions deployed at the largest banks, retailers, and government agencies worldwide

Monitor

Big data **analytics** applied to security

Control

Robust **controls** built into IT fabric, relying on leading IBM technologies across 12+ critical security domains

Apply Insight

World class **research** that finds threats before they impact you

Stage 1: Break-in

1. Break-in
2. Latch-on
3. Expand
4. Gather
5. Exfiltrate

Your Challenge

- Employees are always vulnerable to well-executed phishing attempts
- Even patched machines can be compromised by “zero-day attacks” that leverage previously unknown vulnerabilities
- Antivirus has proven to be largely ineffective against zero-day malware

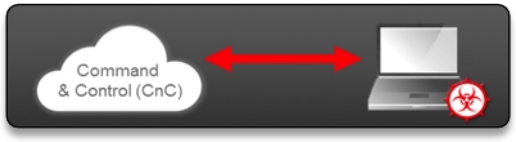
How IBM Can Help

- **IBM Security Network IPS** and **IBM Security Network Protection** help block zero-day exploits using advanced behavioral analysis, and block phishing and malware sites using a database of 13 billion URLs
- **IBM Endpoint Manager** helps limit attack surface by auditing and enforcing compliance with patch and configuration policies

Other Considerations

- Ask your endpoint protection (antivirus) vendor what they provide for advanced detection, and how they detect indicators of compromise
- Consider using a specialized malware detection solution
- Develop and implement a thorough employee education program

Stage 2: Latch-on



1. Break-in
2. **Latch-on**
3. Expand
4. Gather
5. Exfiltrate

Your Challenge

- Once the attacker has breached your perimeter, they need to establish a communication channel back to “home” and create redundant ways to access your network

How IBM Can Help

- **IBM Security QRadar** continuously monitors the network and helps identify anomalous activity in terms of location, applications accessed, and more; logs network activity for future forensic investigations, to help determine extent of breach
- **IBM Security Network IPS** uses advanced behavioral analysis to detect subtle communications with malicious destinations

Other Considerations

- Ask your endpoint protection (antivirus) vendor what they are providing for advanced detection, including detecting indicators of compromise

Stage 3: Expand

Your Challenge

- APTs usually don't infect the host containing target data; thus the attacker needs to find the target data and gain access to it
- They will perform reconnaissance to understand the network and identify high-value assets

How IBM Can Help

- **IBM Security Privileged Identity Manager** helps lock down user accounts with access to high-value systems and data
- **IBM Security QRadar** uses out-of-the-box analytics to look for suspicious network probing – by correlating activity at big data scale
- **IBM Security Host Protection** helps identify suspicious system activity, and inspects and blocks malicious traffic – including connections to encrypted web applications
- **IBM Security AppScan** helps reduce the attack surface of enterprise applications by identifying and prioritizing application vulnerabilities

Other Considerations

- Proactively manage your access policies, grant the minimum rights required, and frequently review user access rights

Stage 4: Gather

Your Challenge

- Once the attacker has compromised your users & gained access to sensitive data repositories, they explore what is available and begin copying target data

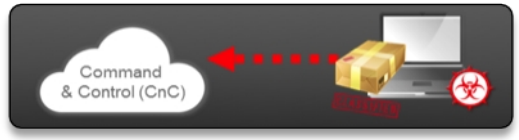
How IBM Can Help

- **IBM InfoSphere Guardium** continuously monitors databases and data warehouses to identify suspicious access and protect sensitive data
- **IBM Security Network IPS** helps block malicious behavior within (and beyond) the network
- **IBM Security Network Protection** controls application access at a granular user and application level
- **IBM Security Privileged Identity Manager** helps enforce access policies

Other Considerations

- Place extra controls and focus around your critical assets and data
- Encrypt & protect data in proportion to its value to you and attackers
- Implement an effective DLP (data loss prevention) strategy

Stage 5: Exfiltrate



Your Challenge

- There are nearly unlimited ways to get acquired data off your network

How IBM Can Help

- **IBM X-Force Threat Intelligence** identifies malicious sites, to help block communications
- **IBM Security QRadar** uses X-Force data to detect traffic to suspect sites; performs activity baselining to help detect anomalous user behavior based on type of activity, volume of transfers, location, etc.
- **IBM Security Network IPS** helps stop encrypted traffic associated with suspicious entities, and sensitive data transmission (eg, credit card numbers)
- **IBM Security Network Protection** tracks and controls application usage in all directions to enforce policies and help prevent data loss

Other Considerations

- Push your Endpoint Protection, Network DLP and Network Security vendors to enhance their detection and blocking of suspicious data transmission

IBM's approach to defending against state-sponsored attacks

Network and Endpoint Security Use adaptive threat protection and endpoint management to reduce risks and fend off attacks

Network Security Use SIEM and adaptive threat protection to help identify and stop attackers from gaining a foothold

Secure Users Leverage strong identity management to enforce access policies and monitor for suspicious behavior

Data Security Embed security deep into data repositories with data activity monitoring; apply fine-grained access controls

Network Security Proactively monitor network traffic for common exfiltration tactics; block in real-time

Security Analytics Leverage Security Intelligence to correlate and analyze activity across the entire enterprise…

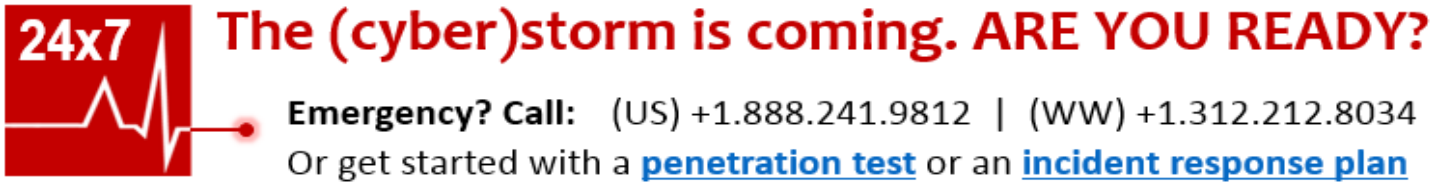
Extend with Big Data capabilities for analyzing unstructured data…

Utilize Emergency Response Services for breach or for assessment of risk

Security **Intelligence**. Think **Integrated**.

What to do if you have been breached

1. Call IBM Emergency Response Services (24x7):



2. Proactively assess risk and reduce future breach likelihood:

- Cyber Incident response training and simulated exercises to determine level of preparedness
- Incident Response Program gap assessment to ensure enterprise readiness and responsiveness when an incident occurs
- Active Threat Assessment as a preemptive service to determine weaknesses requiring remediation
- X-Force threat analysis service is available from IBM experts **24x7**

Key Features

24x7x365 Hotline for clients to call from anywhere worldwide for assistance if they believe they are experiencing an incident

Incident Case Managers who maintain calm, focus, and manage the incident and environment to completion and satisfaction

Advanced tools, expertise and scale for any platform, size client, and location worldwide

Globally collected intelligence applied to each engagement to improve outcomes and efficiencies

Unlimited emergency declarations

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