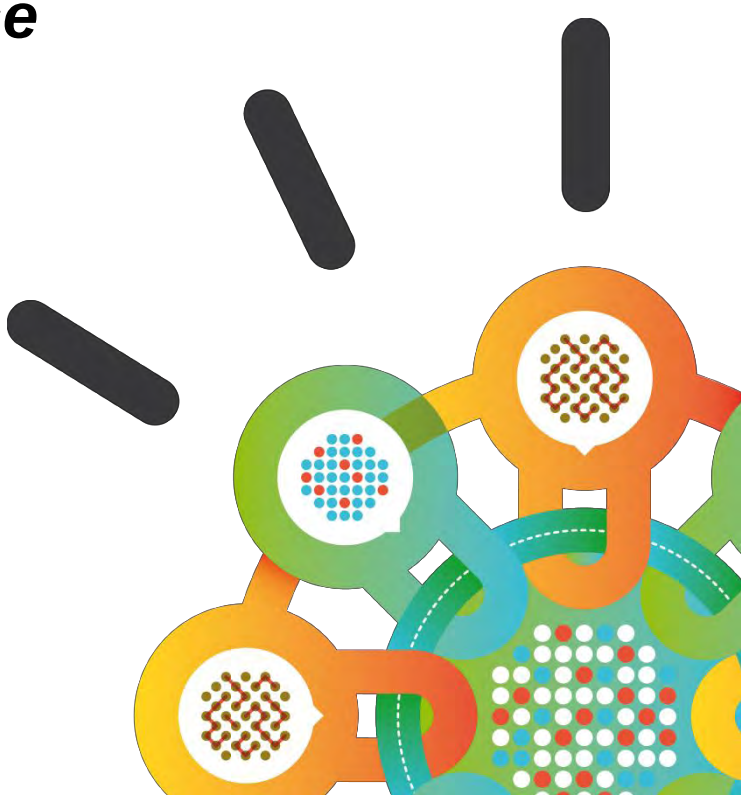
Security Intelligence.
Think Integrated.

IBM Security Strategy

Intelligence, Integration and Expertise

Peter Allor
Security Strategist – Government

IBM Security Systems
February 6, 2014



Motivations and sophistication are rapidly evolving

MOTIVATION

National Security, Economic Espionage

Nation-state actors, APTs
Stuxnet, Aurora, APT-1

Notoriety, Activism, Defamation

Hacktivists
Lulzsec, Anonymous

Monetary Gain

Organized crime
Zeus, ZeroAccess, Blackhole Exploit Pack

Nuisance, Curiosity

Insiders, Spammers, Script-kiddies
Nigerian 419 Scams, Code Red

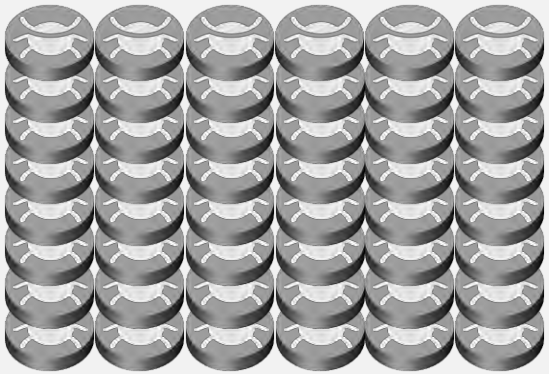
SOPHISTICATION

But our traditional defenses are not keeping up

85 tools from

45 vendors

Source: IBM client example

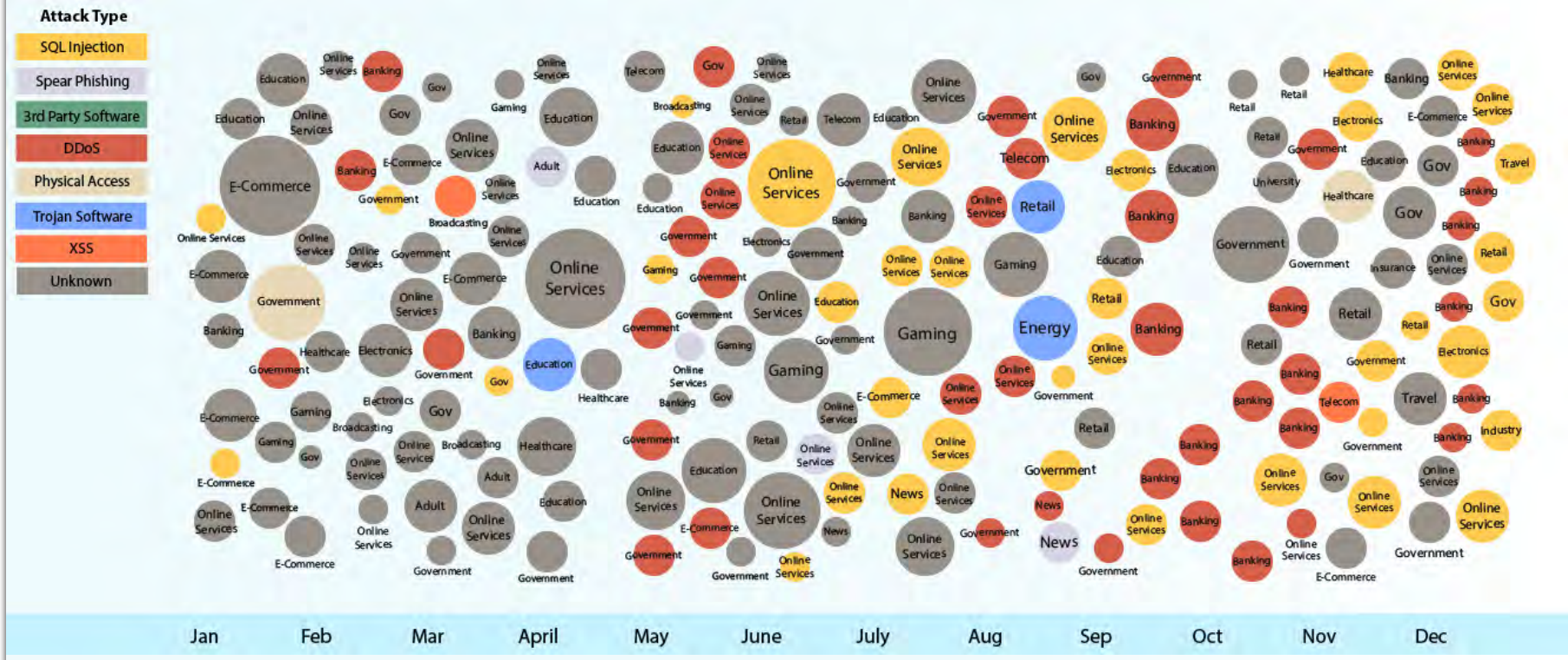


0 out of **46** vendors detected malware

Reported attacks continue to increase

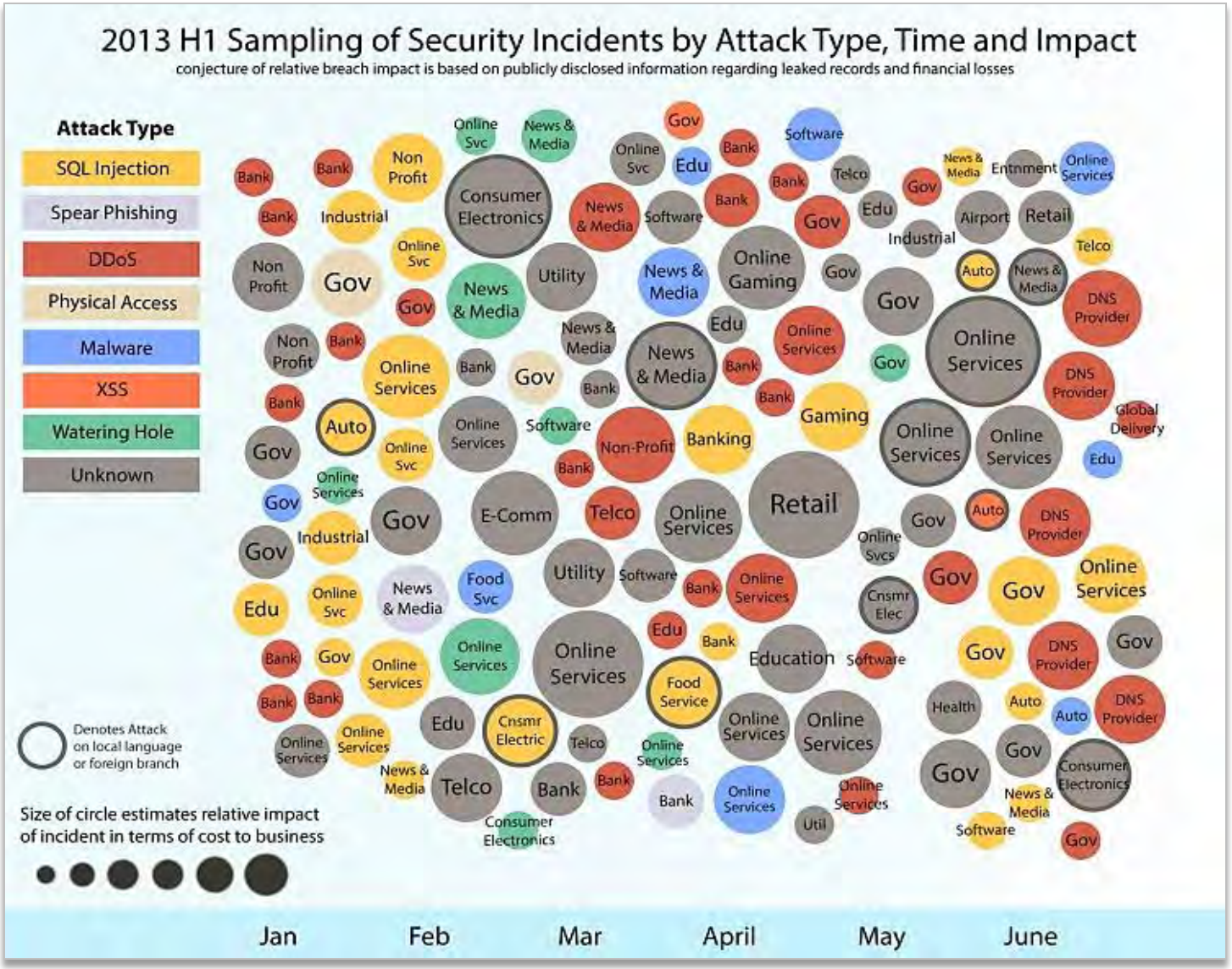
2012 Sampling of Security Incidents by Attack Type, Time and Impact

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



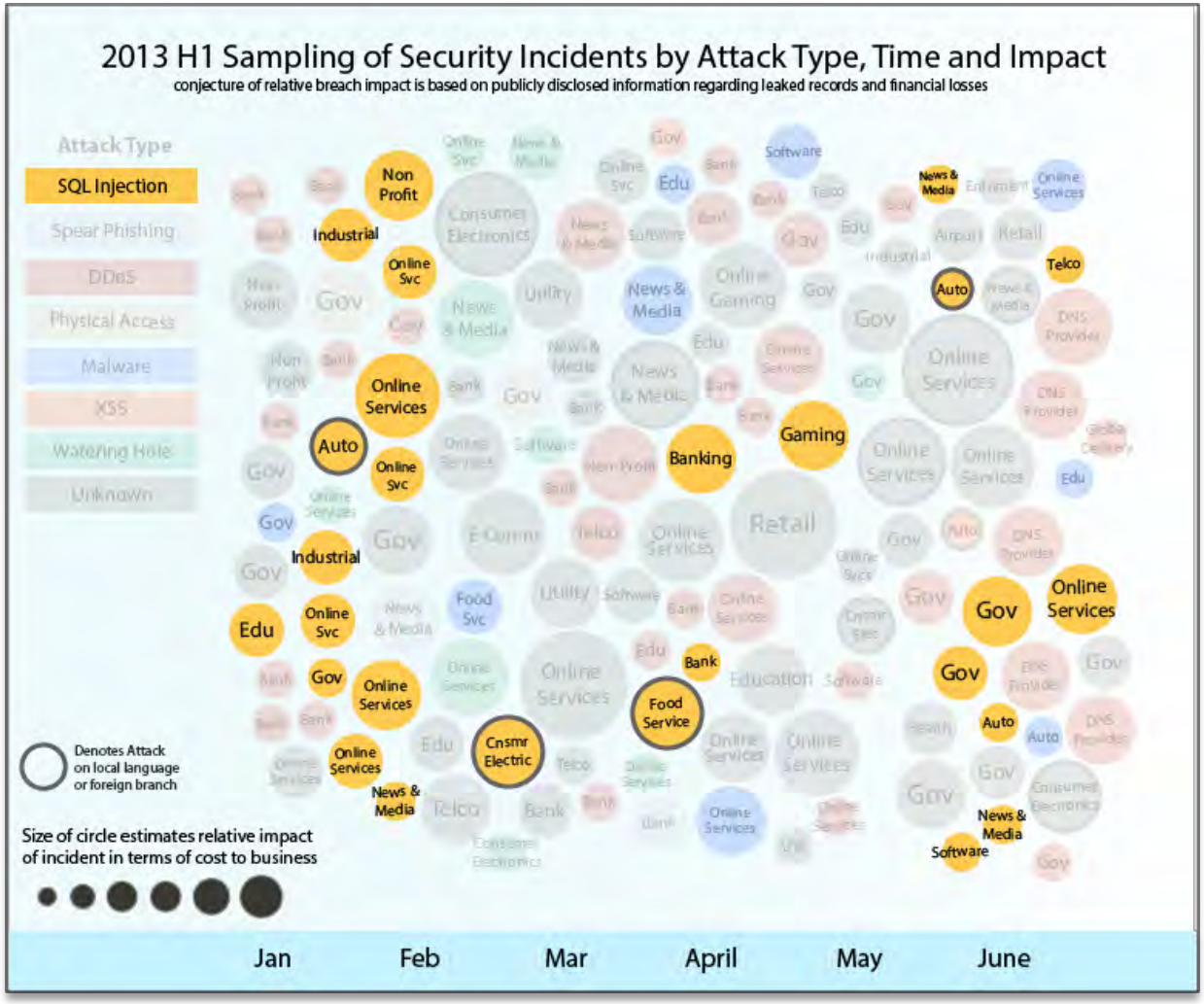
Source: IBM X-Force® Research 2012 Trend and Risk Report

Attack frequency increased to record in H1 2013



Source: IBM X-Force® Research 2013 Trend and Risk Report

SQL Injection
still reliable for breaching databases

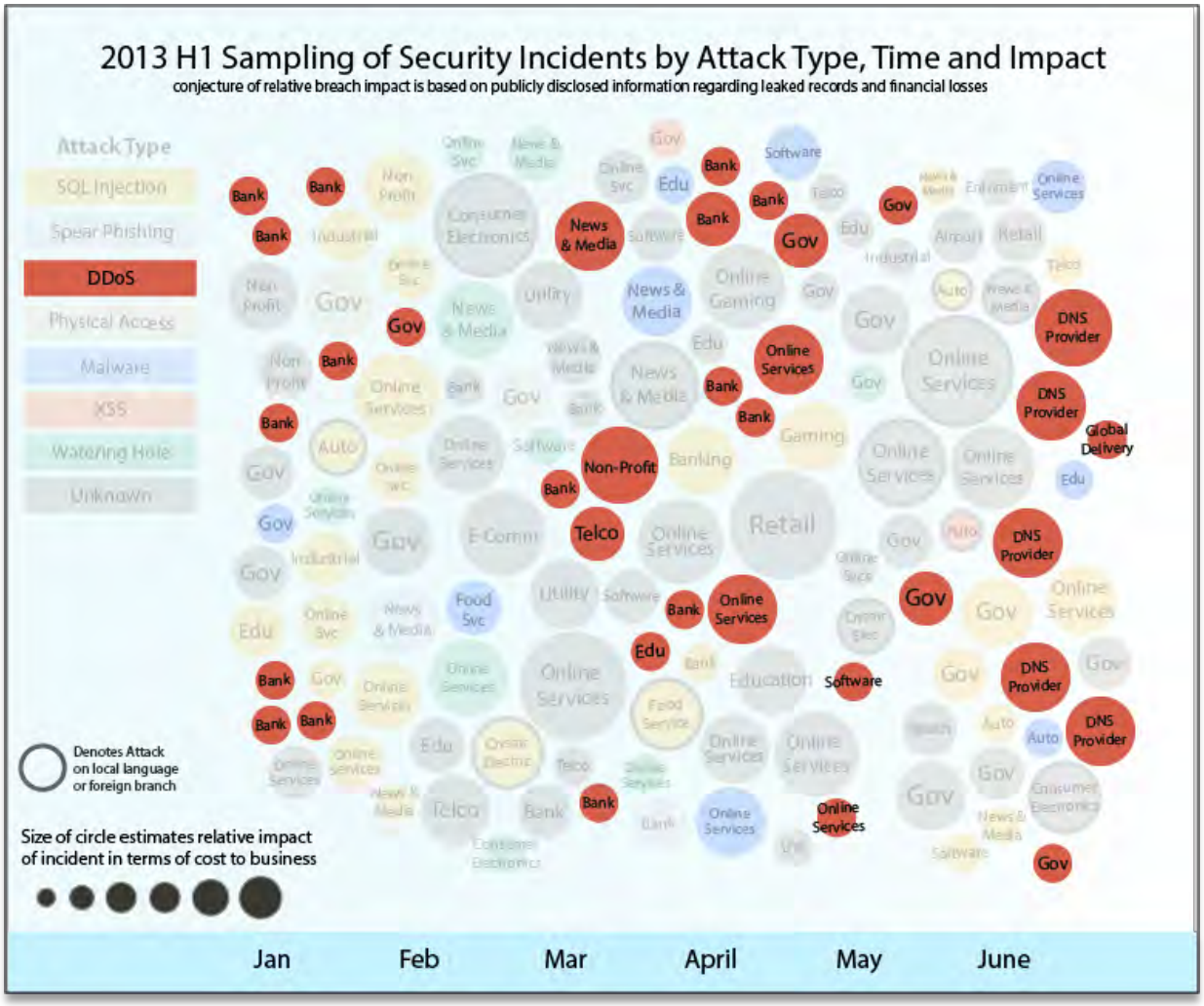


22% of tracked disclosed breaches

Low risk / high reward

- **Old CMS installations**
- **CMS Plugins**
- **Forum software**
- **Other popular 3rd party scripts**

DDoS Attacks
continue to disrupt businesses



High traffic volume as much as

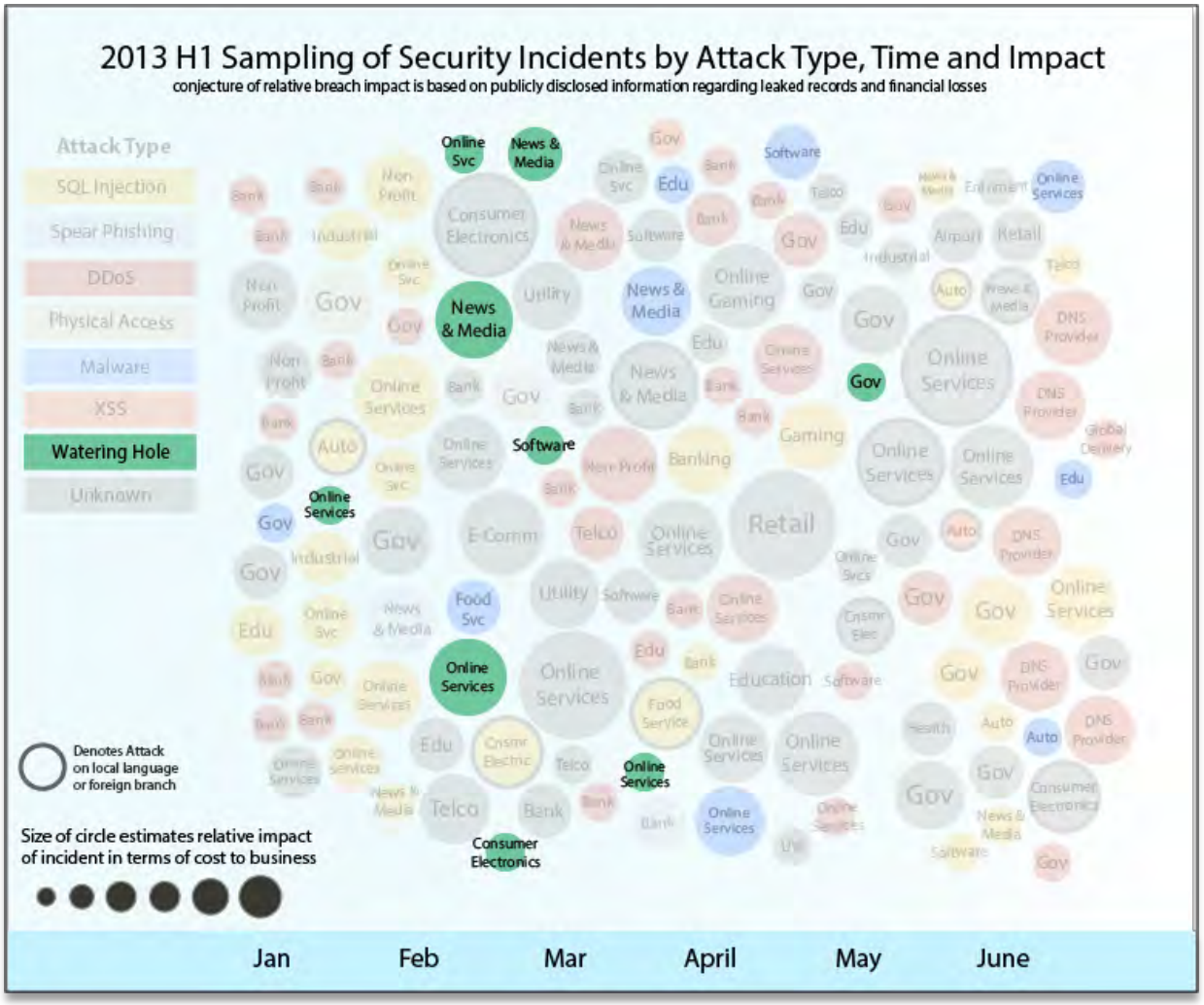
300Gbps

Industries affected:

- **Banks**
- **Governments**
- **DNS Providers**

"Watering Hole"

attacks compromise end user trust



Tainting legitimate sites with zero-day exploits

Targeting Savvy Users

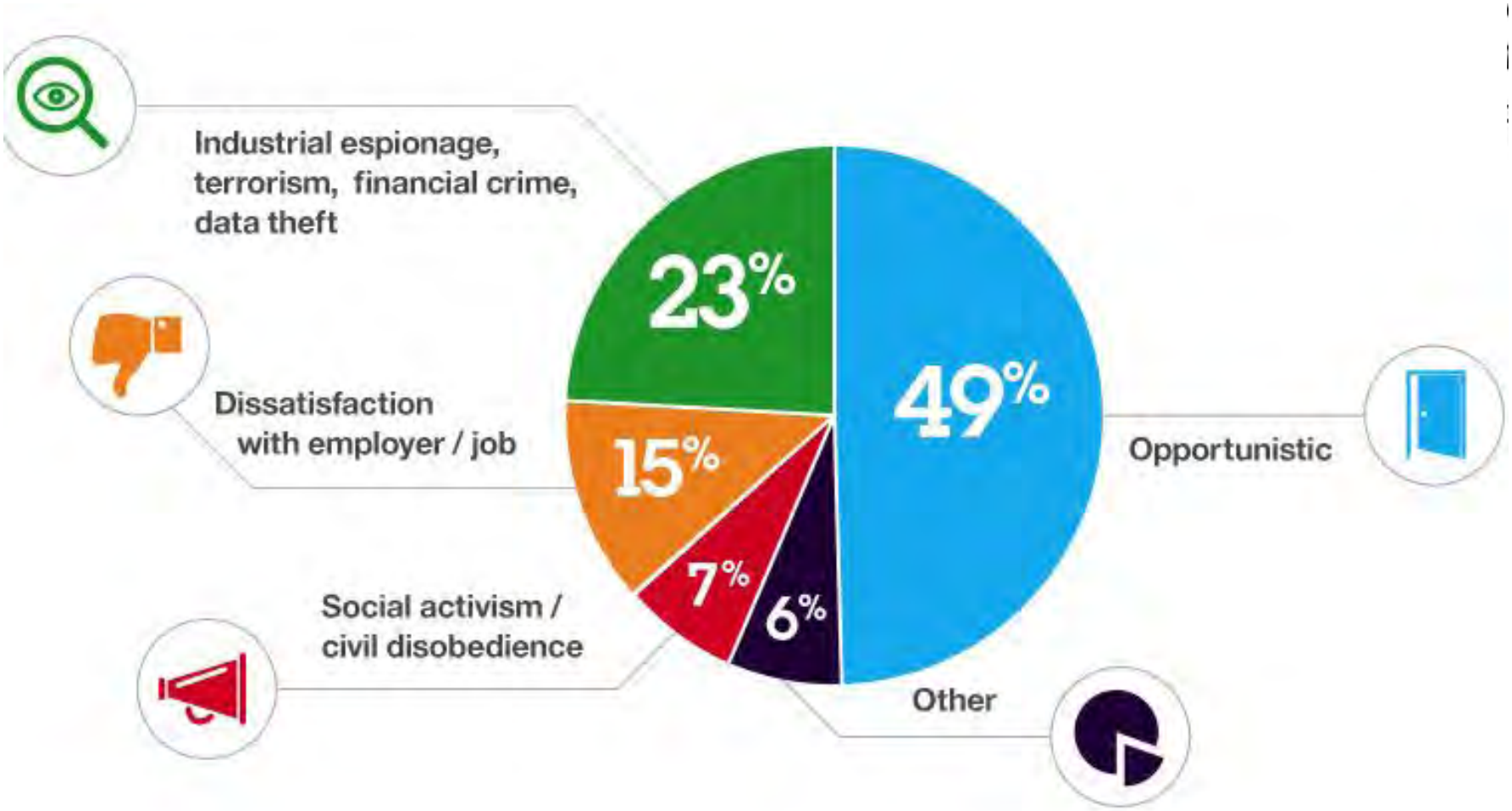
- **Tech company developers**
- **Government Employees**
- **Unsuspecting viewers of trusted sites**

Cyber Espionage

The global reach of the Internet has enabled both phenomenal business growth and unprecedented business risk at the same time.

http://www.abc.net.au/4corners/stories/2013/05/27/3766576.htm

Motivations of the Attacker



Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

Data Explosion and Cloud Growth

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere including new platforms including cloud, virtualization. Everything is everywhere.

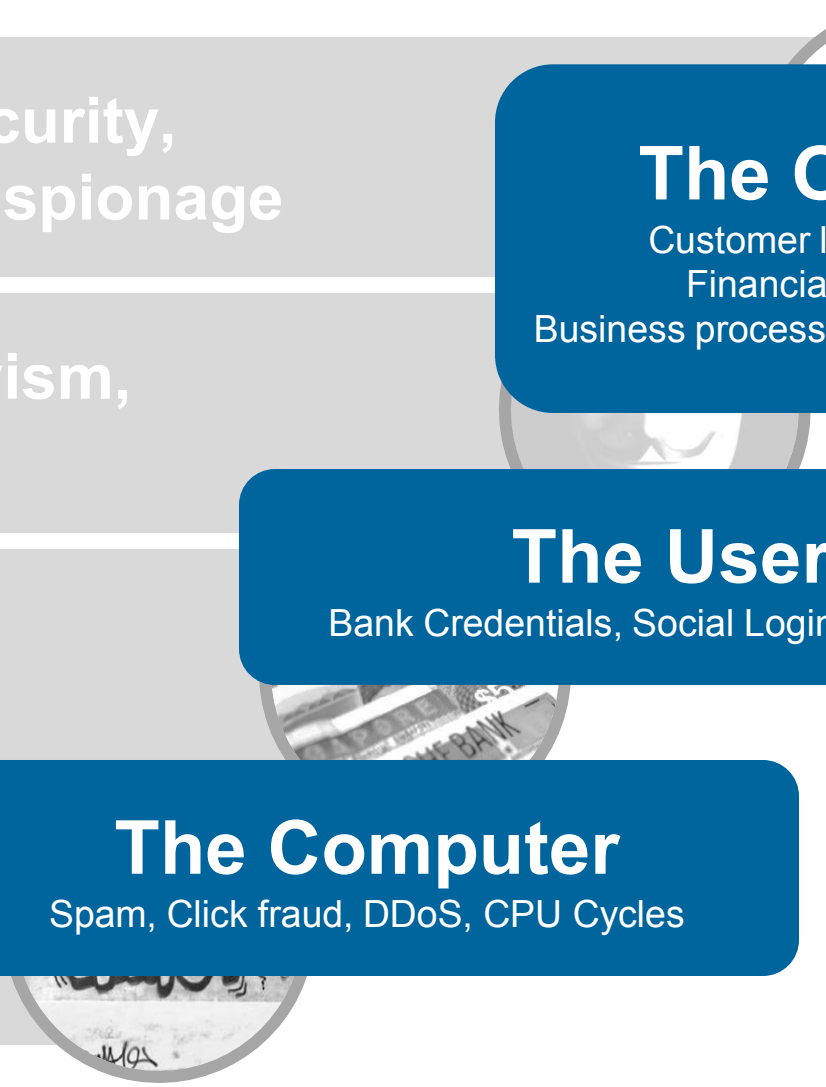
The End Goal

National Security,
Economic Espionage

Press, Activism,
Defamation

Monetary
Gain

Nuisance,
Curiosity



The Organization

Customer lists, Intellectual property,
Financial filings, Product plans,
Business process data, Administrative credentials

The User

Bank Credentials, Social Logins, Ransom

The Computer

Spam, Click fraud, DDoS, CPU Cycles

Collaborative IBM teams monitor and analyze the latest threats

In the first six months of 2013, IBM X-Force:

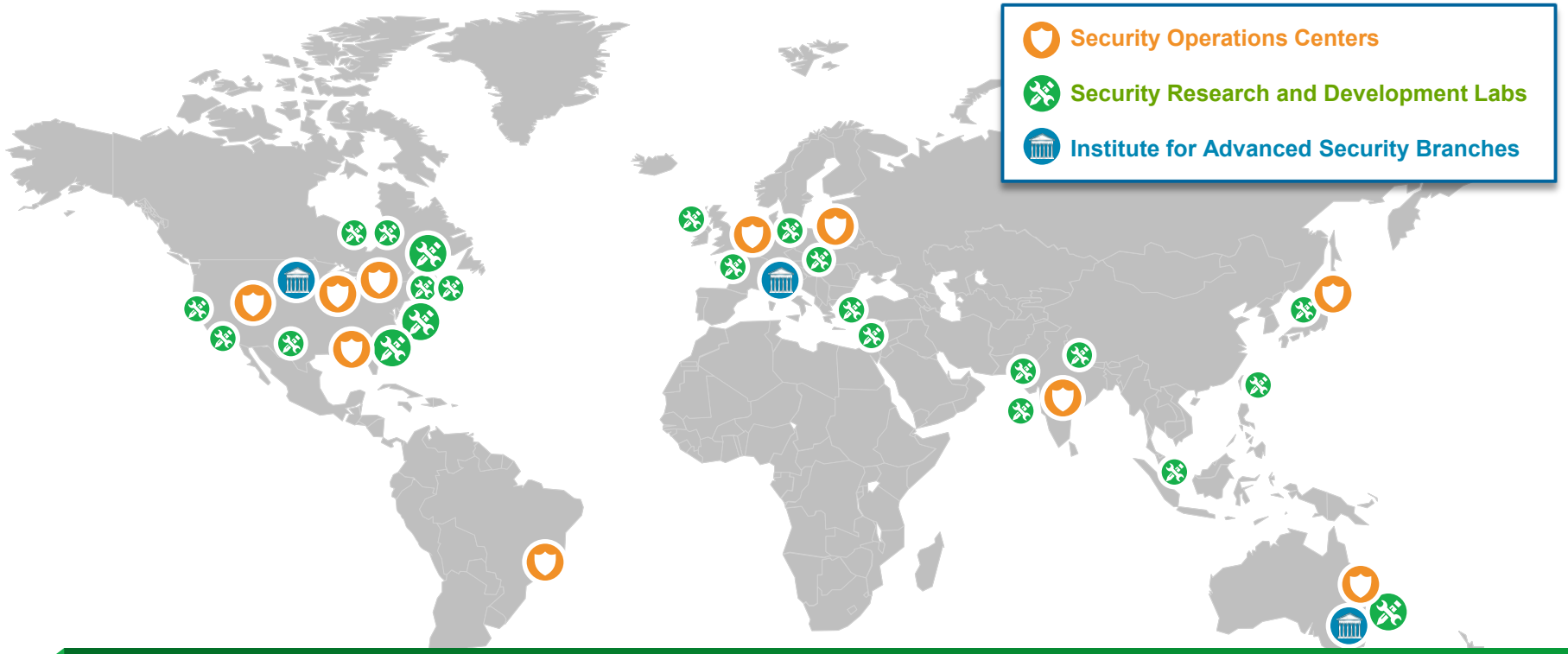
4,100
New security vulnerabilities analyzed

900M
New web pages and images analyzed.
20 billion since 1999.

27M
New or updated entries in the IBM web filter database.
81 million in total.

180m
New, updated, or deleted signatures in the IBM spam filter database.
40 million in total.

At IBM, the world is our security lab



6,000 IBM researchers, developers, and subject matter experts ALL focused on security

More than **3,000** IBM security patents

v13-01

5 Most Targeted Industries

Manufacturing

26.5%

Finance & Insurance

20.9%

Information & Communication

18.7%

Health & Social Services

7.3%

Retail & Wholesale

6.6%

Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

Why do Breaches Happen

Source: *IBM Security Services 2013 Cyber Security Intelligence Index*

2012 Major Trends

40% Security Incidents

14% Web Vulnerabilities

20% SPAM within 2012

53% Web Vulns are XSS

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

ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new motivations from cyber crime to state sponsored to terror inspired.

2012 Vulnerabilities and Exploits

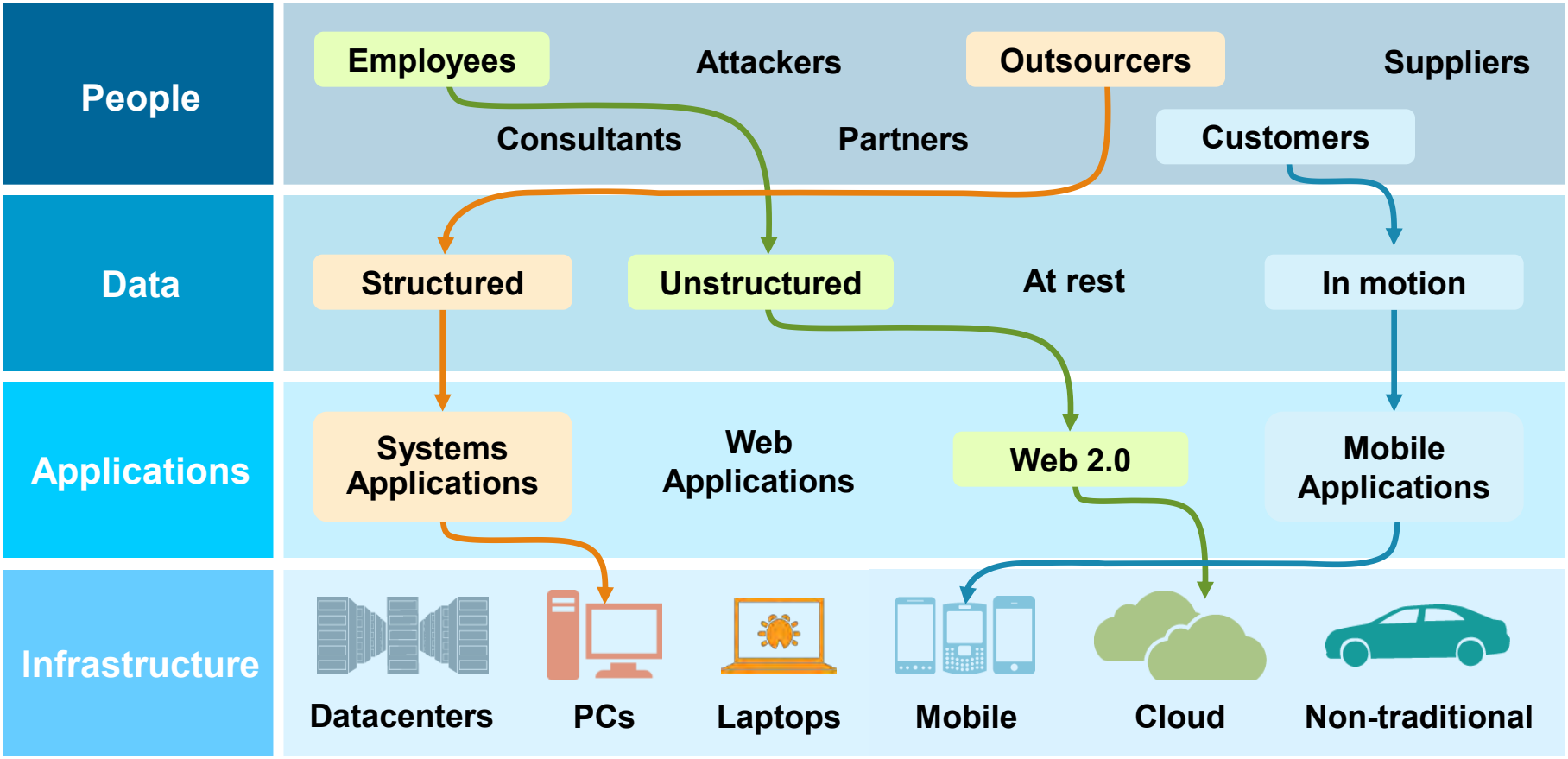
8,168 Public Vulnerabilities

864 Public Exploits

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

A new approach to security is needed

Security challenges are a complex, four-dimensional puzzle…



…that requires a new approach

Thinking differently about security

	Then		Now
People	Administration		Insight
Data	Basic-control		Laser-focused
Applications	Bolt-on		Built-in
Infrastructure	Thicker walls		Smarter defenses

Analyze to build Intelligence

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

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

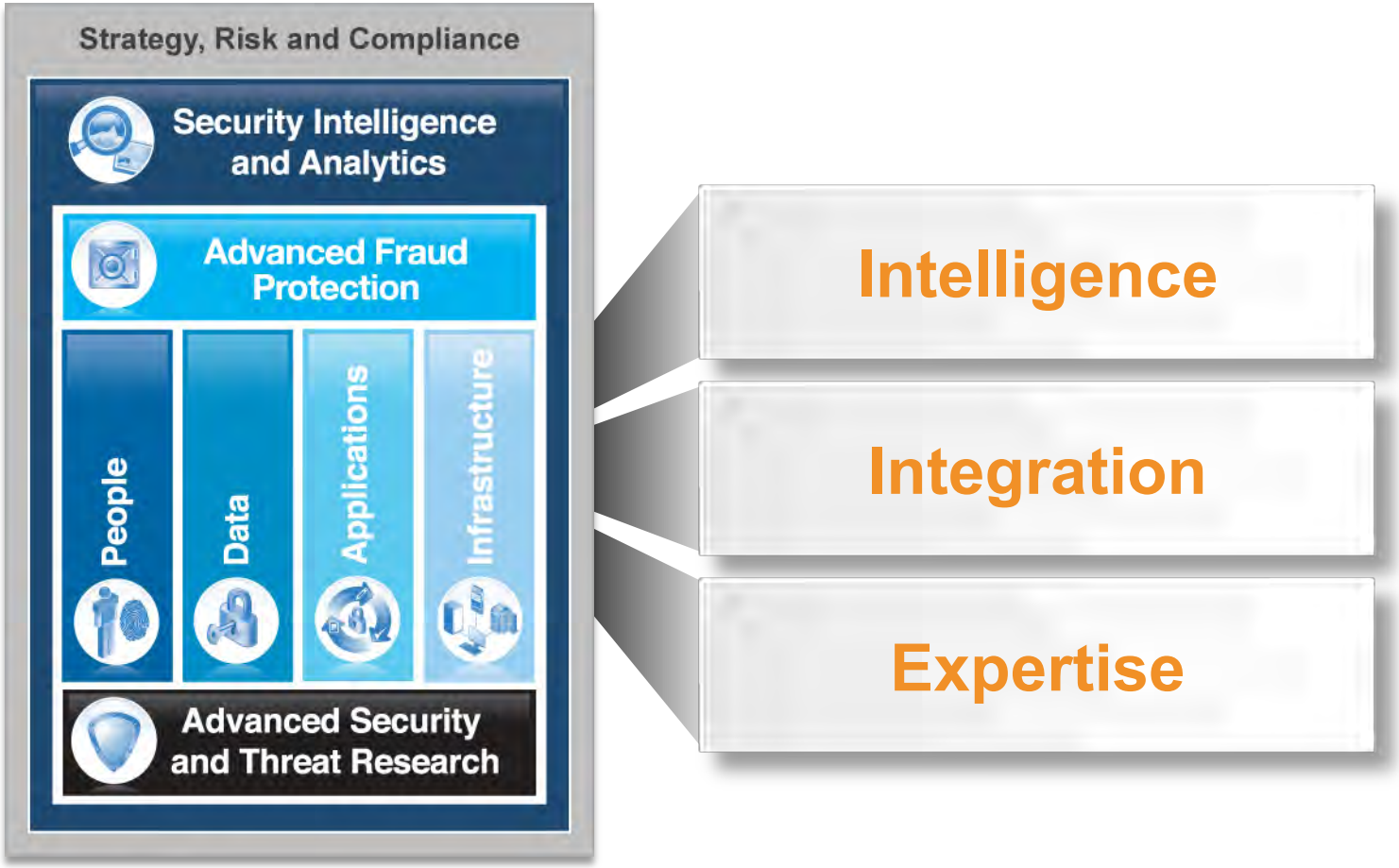
Detect, Analyze & Remediate

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

Broad **Targeted**

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



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

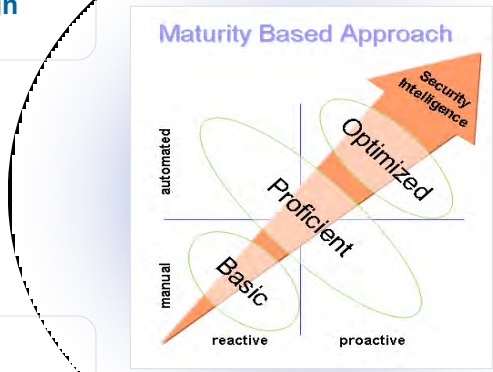
5. Take a Hygienic Approach to Managing Infrastructure

6. Control Network Access

4. Secure Services, By Design

7. Address New Complexity of Cloud and Virtualization

3. Secure the Workplace of 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

Approach aligned with corporate initiatives – not an afterthought

Ongoing series of articles: www.ibm.com/smarter/cai/security

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

Key takeaways for CISOs

Don’t forget the basics

scanning, patching, configurations, passwords

Social Defense needs Socialization

educate users and engender suspicion

Defragment your Mobile posture

constantly apply updates and review BYOD policies

Optimize ahead of Attackers

identify critical assets, analyze behavior, spot anomalies

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.

Thank You

www.ibm.com/security