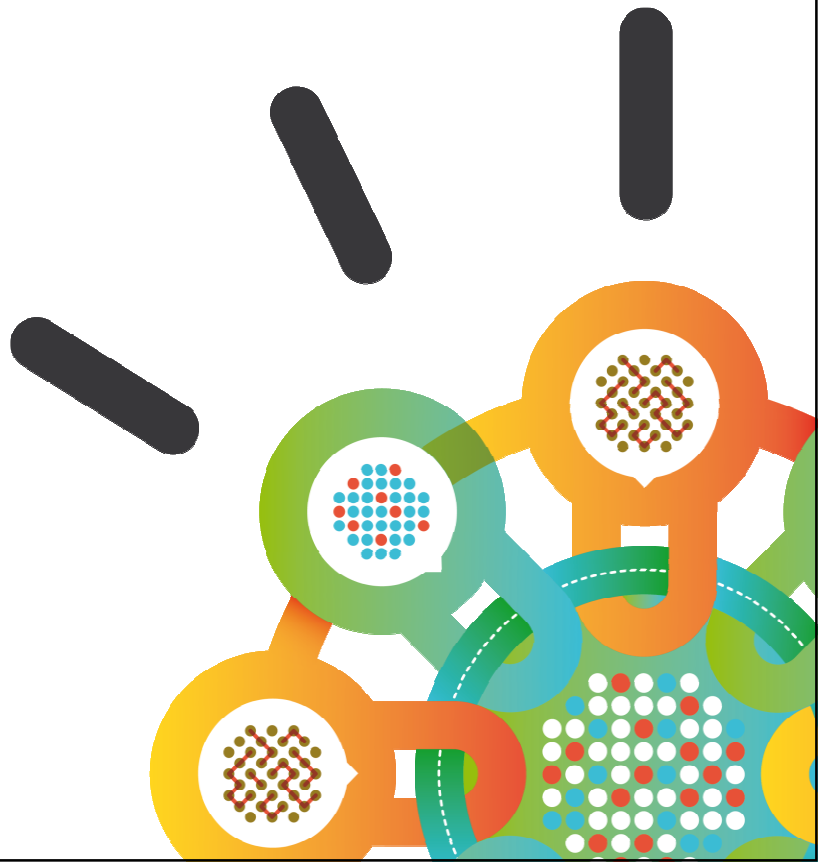
Defending Against Cyber Threats with Intelligent, Security-ready Infrastructure

Shelley Westman
IBM Vice President
and Business Line Executive, Security

June 25, 2013

The changing dynamics of securing the Enterprise



Businesses are under increasing pressure to deliver transformative value—with fewer resources

Increased risk

40%

of Fortune 500 and popular web sites contain a vulnerability[2]

Budgetary constraints

71%

of the average IT budget is dedicated to ongoing operations[4]

Mobile in the enterprise

90%

of organizations will support corporate apps on personal devices by 2014[6]

Social business

74%

of enterprises use social media today to communicate with clients[7]

Innovation in the cloud

60%

of chief information officers view cloud computing as critical to their plans[5]

Exploding data growth

2.7ZB

of digital content in 2012, a 50% increase from 2011[3]

Aging Infrastructure

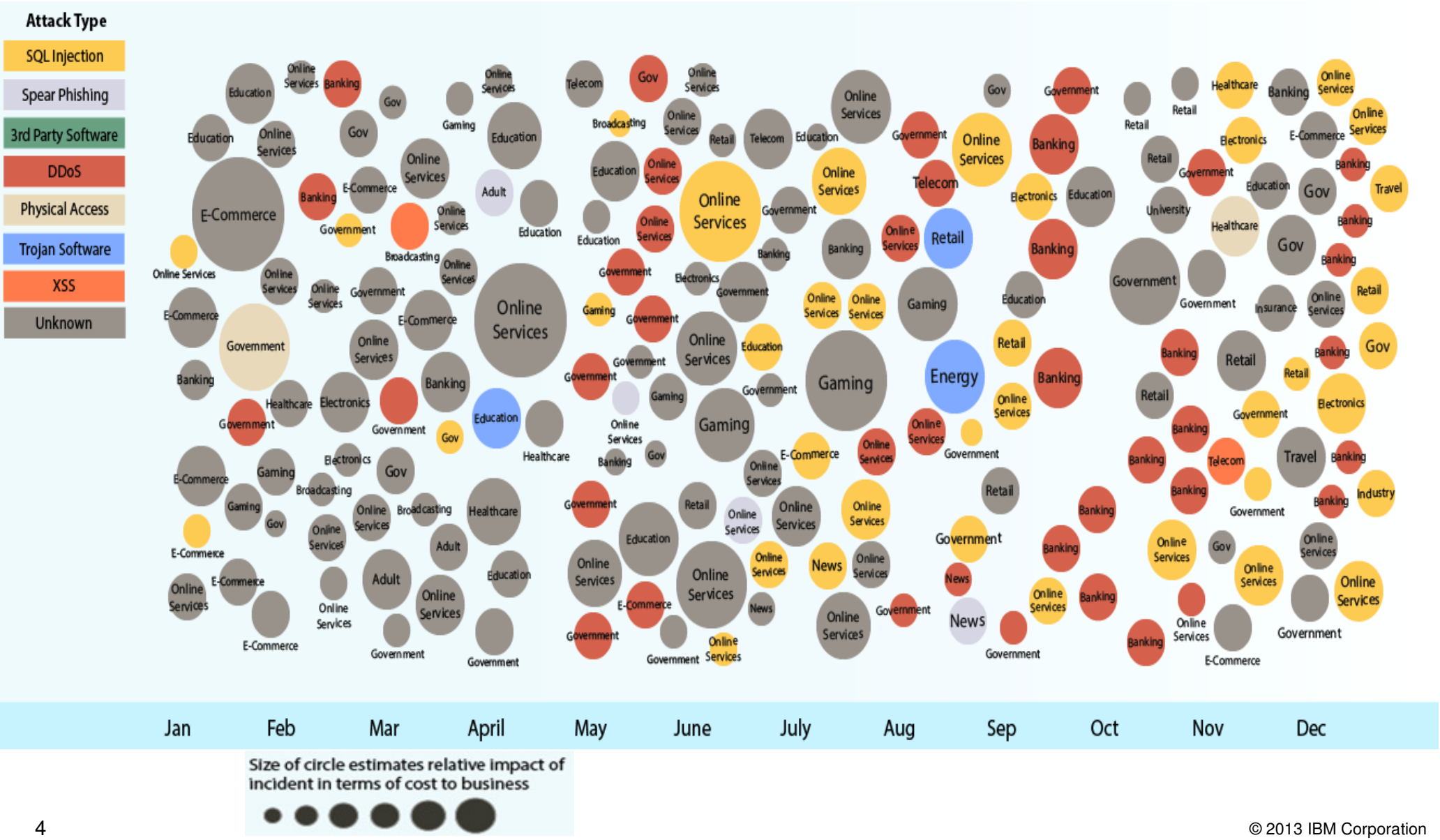
71%

of data centers are over 7 years old[1]

Sources: [1]The Essential CIO: Insights from the Global Chief Information Officer Study, May 2011, [2]IBM X-Force® Mid-year 2011 Trend and Risk Report, September 2011, [3]IDC, "IDC Predictions 2012: Competing for 2020" by Frank Gens December 2011, IDC #231720, Volume:1, [4]Based on IBM Research, [5]McKinsey How IT is managing new demands 2011, [6]Gartner predicts that by 2014, "90% of organizations will support corporate applications on a personal devices.", [7]Forrsights Business Decision-Makers Survey, Q4 2011

2012: The explosion of breaches continues!

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



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

The almost daily headlines continue into 2013….

The Washington Post

More companies reporting cybersecurity incidents

By Ellen Nakashima and Danielle Douglas, Published: March 1

BANK INFO SECURITY®

DDoS Hacktivists: No U.S. Bank is Safe

The Atlantic wire what matters now

How to Survive the Year of the Hack

By Rebecca Greenfield | The Atlantic Wire – Fri, Mar 29, 2013

The New York Times

Retailers Track Employee Thefts in Vast Databases

By STEPHANIE CLIFFORD and JESSICA SILVER-GREENBERG
Published: April 2, 2013 | 5 Comments

Attacks Used the Internet Against Itself to Clog Traffic

By JOHN MARKOFF and NICOLE PERLROTH
Published: March 27, 2013

The New York Times

Cyberattacks Seem Meant to Destroy, Not Just Disrupt

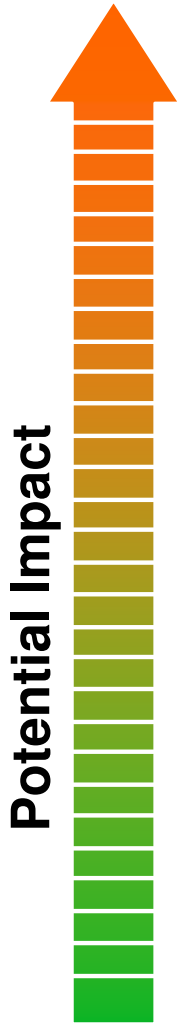
By NICOLE PERLROTH and DAVID E. SANGER
Published: March 28, 2013 | 30 Comments

REUTERS

Quarter of U.S. firms in China face data theft: business lobby

By Michael Martina | Reuters – Fri, Mar 29, 2013

Today's threats are more sophisticated



Threat	Type	% of Incidents	Threat Profile
Advanced, Persistent Threat / Mercenary	• National governments • Organized crime • Industrial spies • Terrorist cells	23%	• Sophisticated tradecraft • Foreign intelligence agencies, organized crime groups • Well financed and often acting for profit • Target technology as well as information • Target and exploit valuable data • Establish covert presence on sensitive networks • Difficult to detect • **Increasing in prevalence**
Hacktivist	• "White hat" and "black hat" hackers • "Protectors of "Internet freedoms"	15%	• Inexperienced-to-higher-order skills • Target known vulnerabilities • Prefer denial of service attacks BUT use malware as means to introduce more sophisticated tools • Detectable, but hard to attribute • **Increasing in prevalence**
Opportunist	• Worm and virus writers • Script Kiddie	7%	• Inexperienced or opportunistic behavior • Acting for thrills, bragging rights • Limited funding • Target known vulnerabilities • Use viruses, worms, rudimentary Trojans, bots • Easily detected
Inadvertent Actor	• Insiders - employees, contractors, outsourcers	49%	• No funding • Causes harm inadvertently by unwittingly carrying viruses, or posting, sending or losing sensitive data • Increasing in prevalence with new forms of mobile access and social business

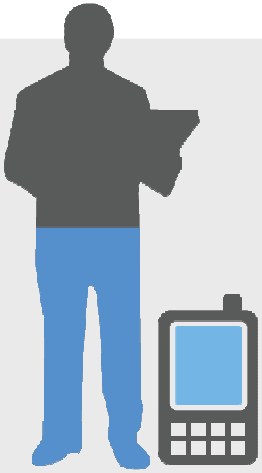
Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434

In IBM's recent 2012 Chief Information Security Officer Study, security leaders shared their views on how the landscape is changing

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

The study also revealed that Security Leaders must have a Strategic Voice in the company

And their roles are evolving with growing **authority, accountability** and **impact** across the enterprise.

Influencers

Confident and prepared, influence the business strategically

Protectors

Less confident, prioritize security strategically but lack necessary structural elements

Responders

Least confident, focus largely on protection and compliance

How they differ

IBM Center for Applied Insights, www.ibm.com/smarter/cai/security

We see the Security market shifting

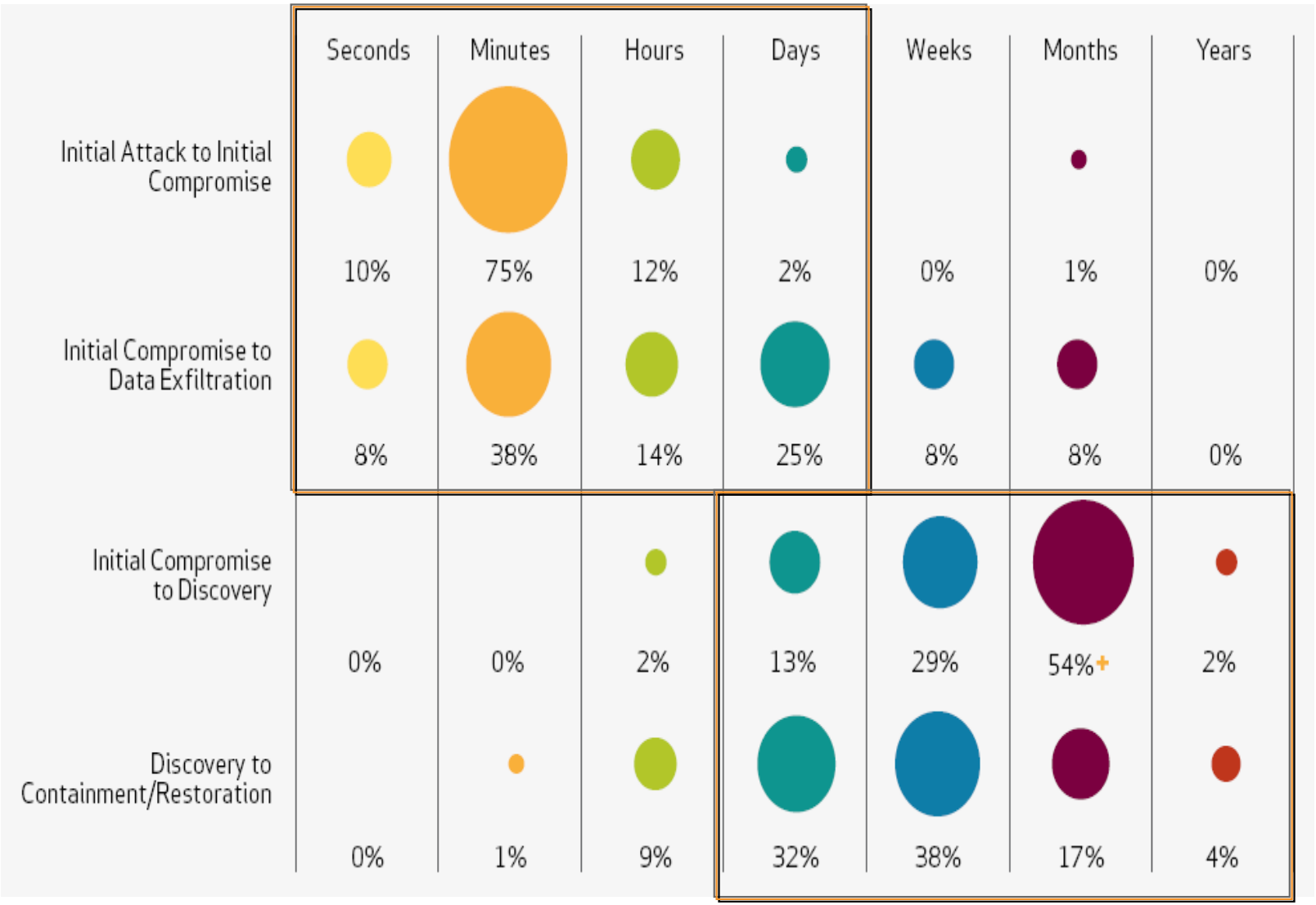
	Traditional Focus *Governance and Compliance*	**Emerging Focus** *Risk Management*
Purchase priority	Compliance	Security
Security strategy	React when breached	Continual management
Speed to react	Weeks/months	Real-time
Executive reporting	None	Operational KPIs
Data tracking	Thousands of events	Millions of events
Network monitoring	Server	All devices
Employee devices	Company issued	Bring your own
Desktop environment	Standard build	Virtualization
Security enforcement	Policy	Audit
Endpoint devices	Annual physical inventory	Automatically managed
Security technology	Point products	Integrated
Security operations	Cost Center	Value Driver

Source: IBM Client Insights

It only takes minutes from attack to comprise but months to discover and recover. **Early detection** and **rapid response** are the best defense

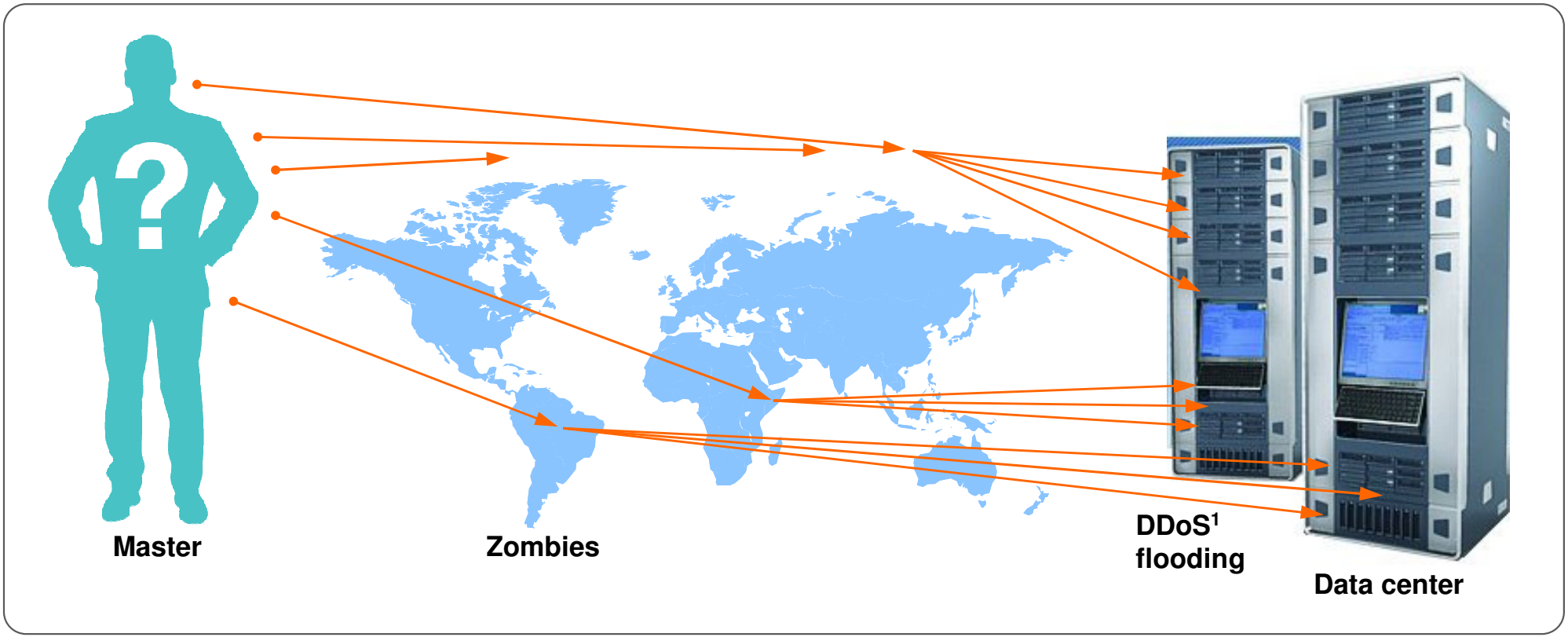
Compromises take days or more to discover in 96% of cases…

…and weeks or more to contain in over 91% of cases



An example of a denial-of-service attack (DDoS).

- Hacktivist or other adversary launches concurrent attacks from multiple worldwide locations
- Attacks intended to saturate network connections and disable web presence
- Results in lost business opportunities and brand impact



[1]Distributed denial of service (DDoS)

Techniques used by attackers are bypassing traditional defenses

Advanced

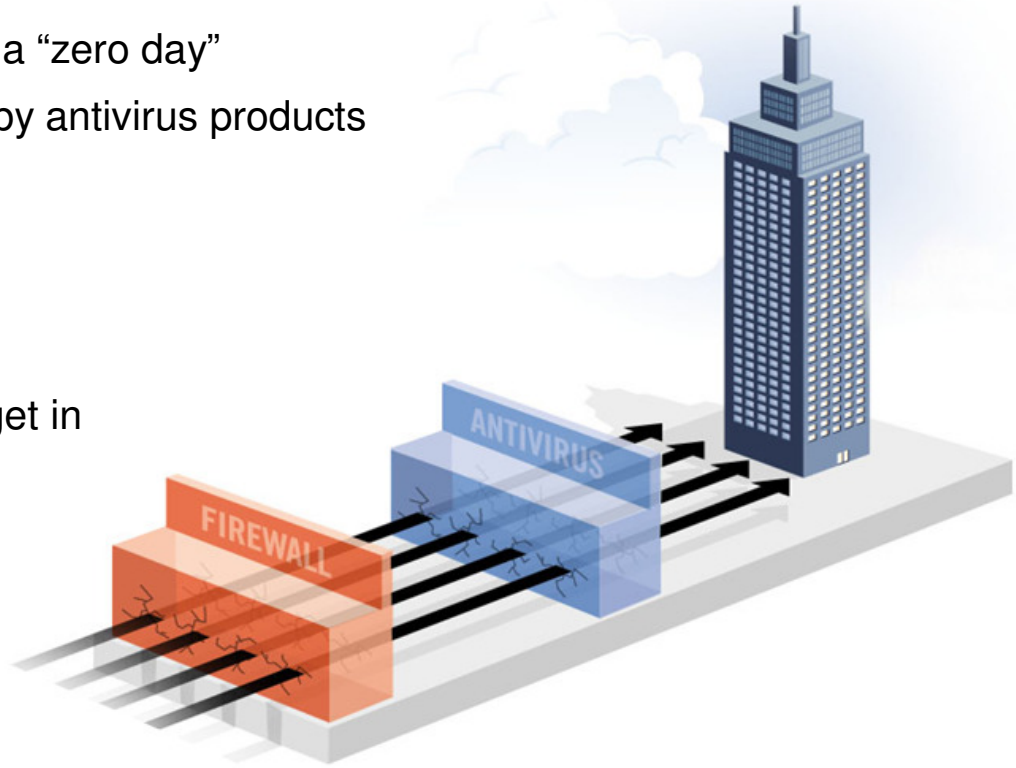
- Using exploits for unreported vulnerabilities, aka a “zero day”
- Advanced, custom malware that is not detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

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

Threat

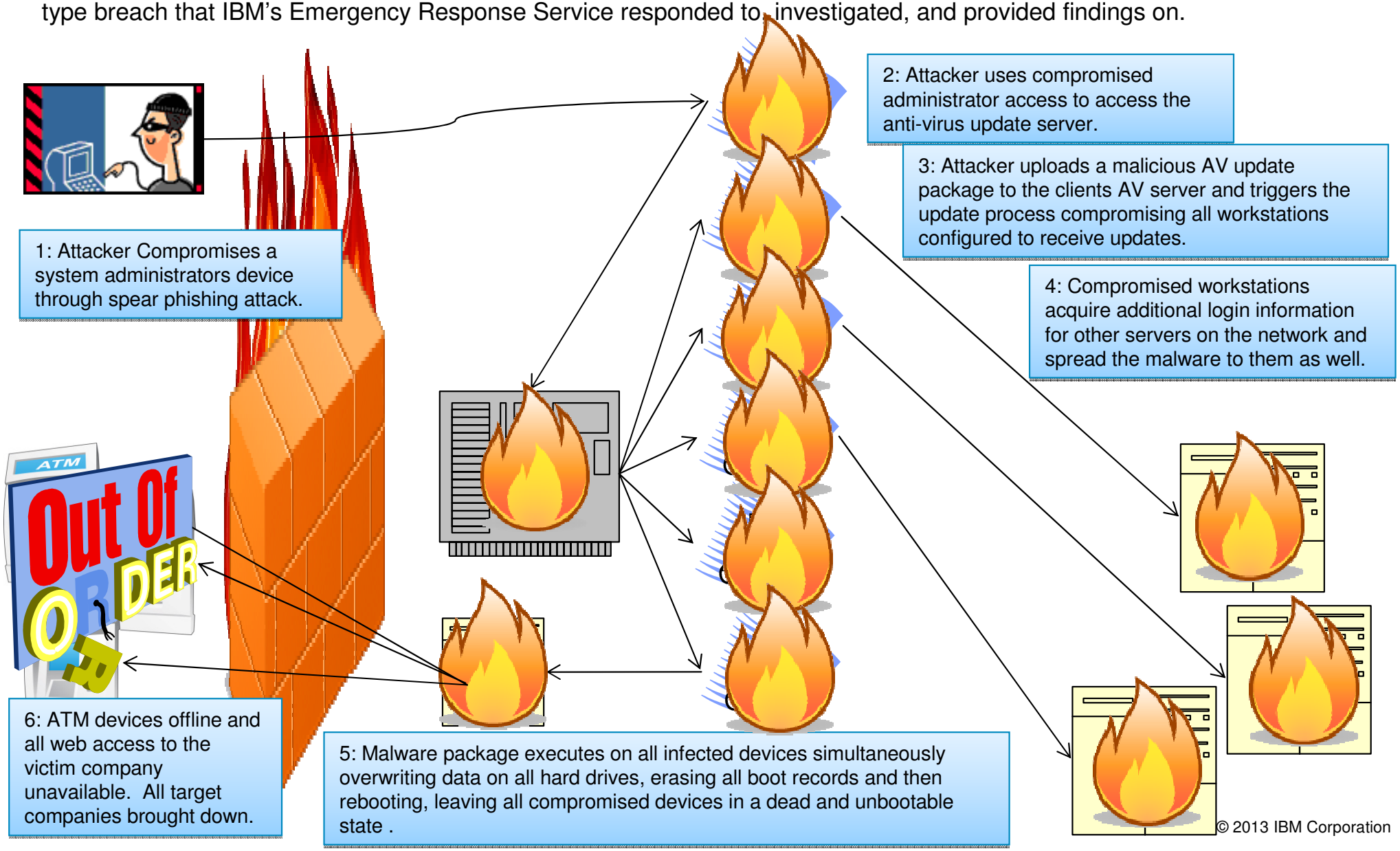
- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are actually “out to get you”



These methods have eroded the effectiveness of traditional defenses including firewalls, intrusion prevention systems and antivirus - ***leaving holes in the network***

Detailed Example of an Advanced Persistent Threat

In the below illustration is an example of a recent event that has been categorized as an Advanced Persistent Threat or APT type breach that IBM's Emergency Response Service responded to, investigated, and provided findings on.



It's not just the private sector that is concerned…..

- U.S. Intelligence chiefs put cyber attacks as number one threat to U.S.
- NSA chief: Hackers causing "the greatest transfer of wealth in history"
- Iran suspected of coordinated DDoS attacks against U.S. banks
- Destructive attacks: South Korea, Saudi Aramco

Did You Know?

Top reasons attacks are possible:

- End user didn't think before clicking
- Weak Password/default password
- Insecure configuration
- Use of legacy/un-patched hardware or software
- Lack of basic network security protection of segmentation

Magnitude of attacks:

2,641,350 security events the average company faces per week

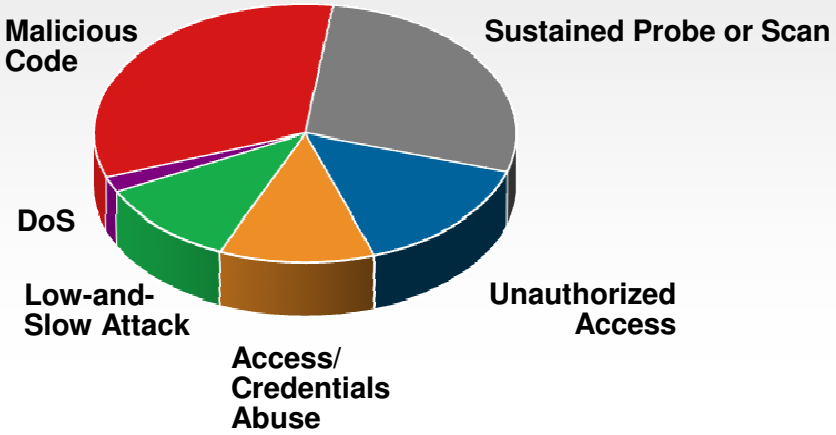
62 Security Incidents the average company experiences per week

6 Security incidents the mature company faces per week

The top 7 attacked industries:

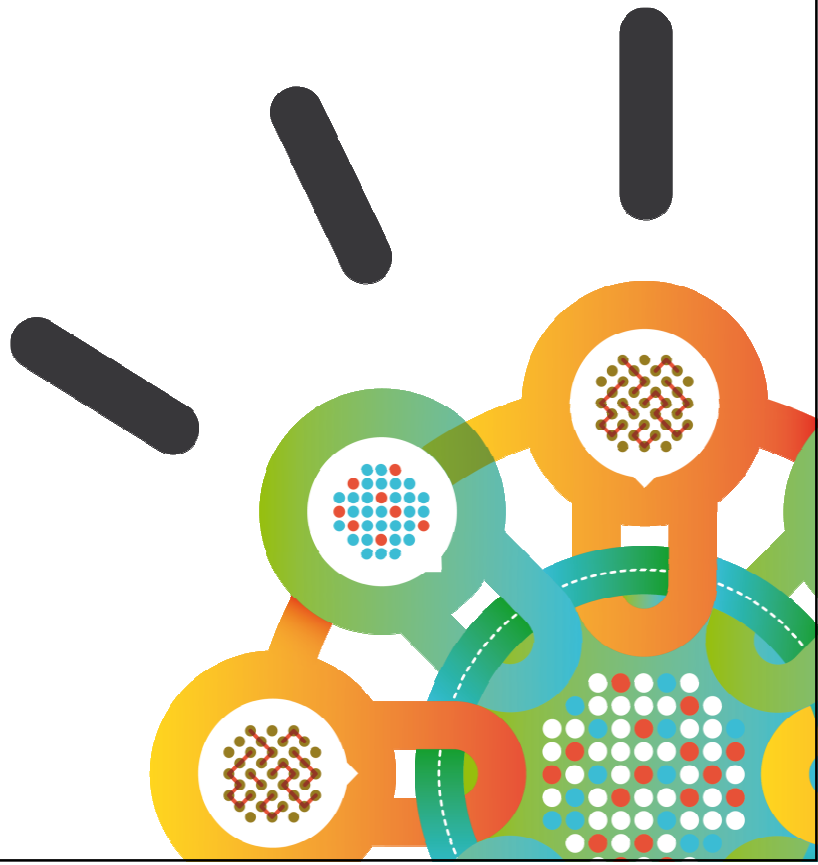
Health & Social Services
Transportation
Hospitality
Finance & Insurance
Manufacturing
Real Estate
Mining, Oil & Gas

What IBM Sees: *Categories of Attack*

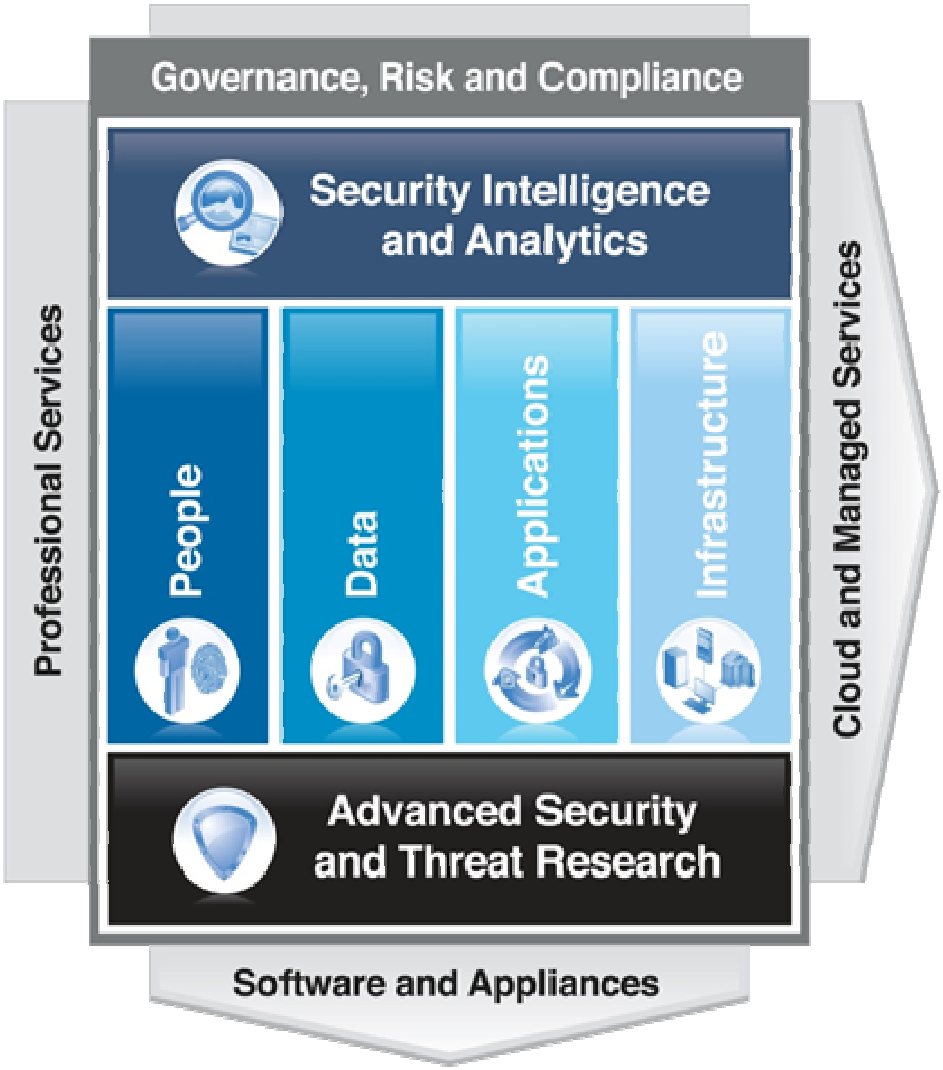


Source: IBM Cybersecurity Intelligence & Response Team Scorecard 2012

How do we solve this?



IBM's security framework…



Intelligence Integration Expertise

Security Intelligence and Analytics
Optimize security management with additional context, automation and integration across domains

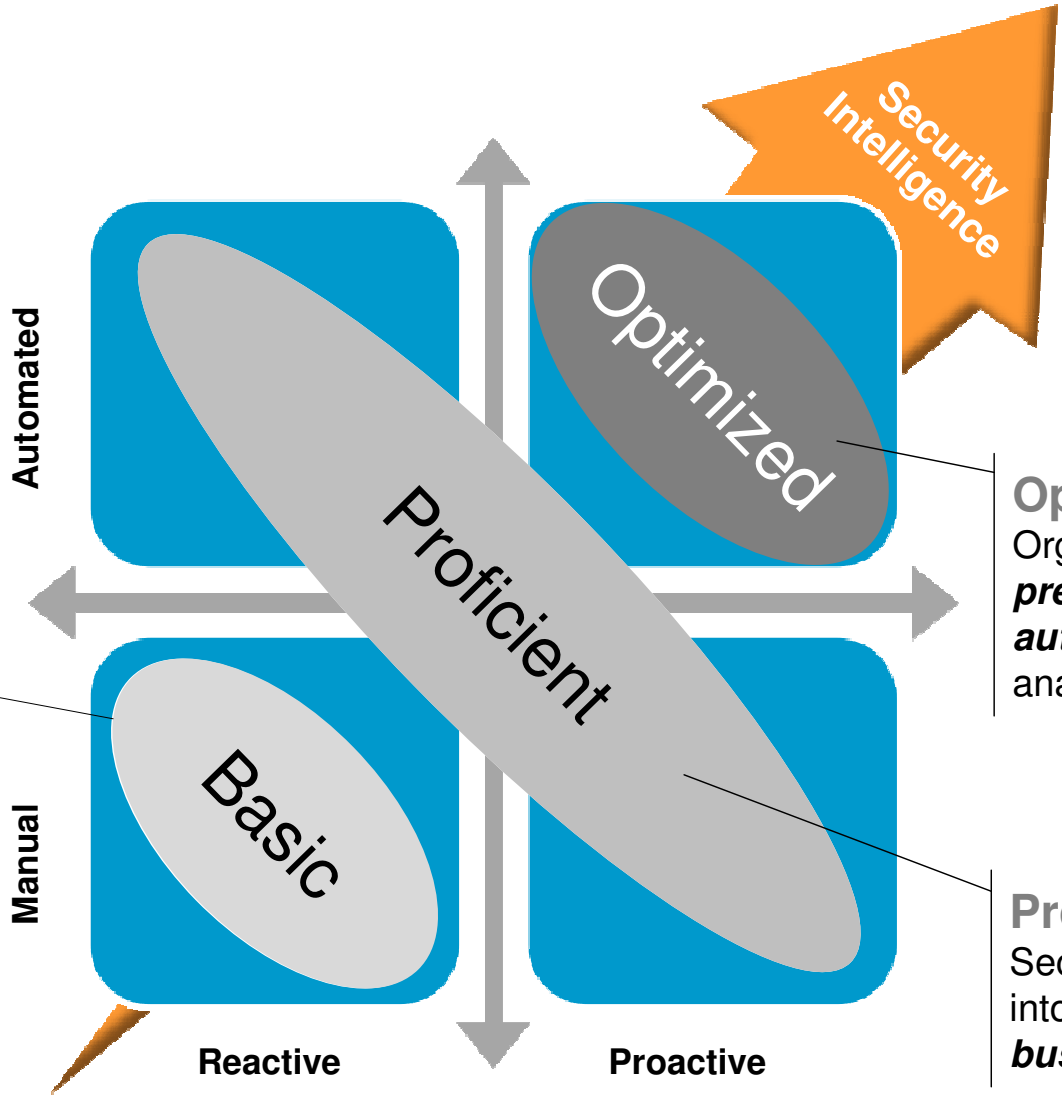
People
Mitigate the risks associated with user provisioning and access to corporate resources

Data
Understand, deploy, and properly test controls for access to and usage of sensitive data

Applications
Keep applications secure, protected from malicious or fraudulent use, and hardened against failure

Infrastructure
Help protect and maintain compliance of networks, servers, storage, endpoints and mobile devices

IBM's point of view on Security



Optimized
Organizations use ***predictive and automated*** security analytics

Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Proficient
Security is layered into the ***IT fabric*** and ***business operations***

Thinking differently about security

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

Collect and Analyze Everything

Advanced Research

Domain	IP Address	File Checksum
dogpile.com	**117.0.178.252**	c69d172078b439545dfff28f3d3aacc1
kewww.com.cn	83.14.12.218	**51e65e6c798b03452ef7ae3d03343d8f**
ynnsuue.com	94.23.71.55	**6bb6b9ce713a00d3773cfcecef515e02**

Monitor Everything

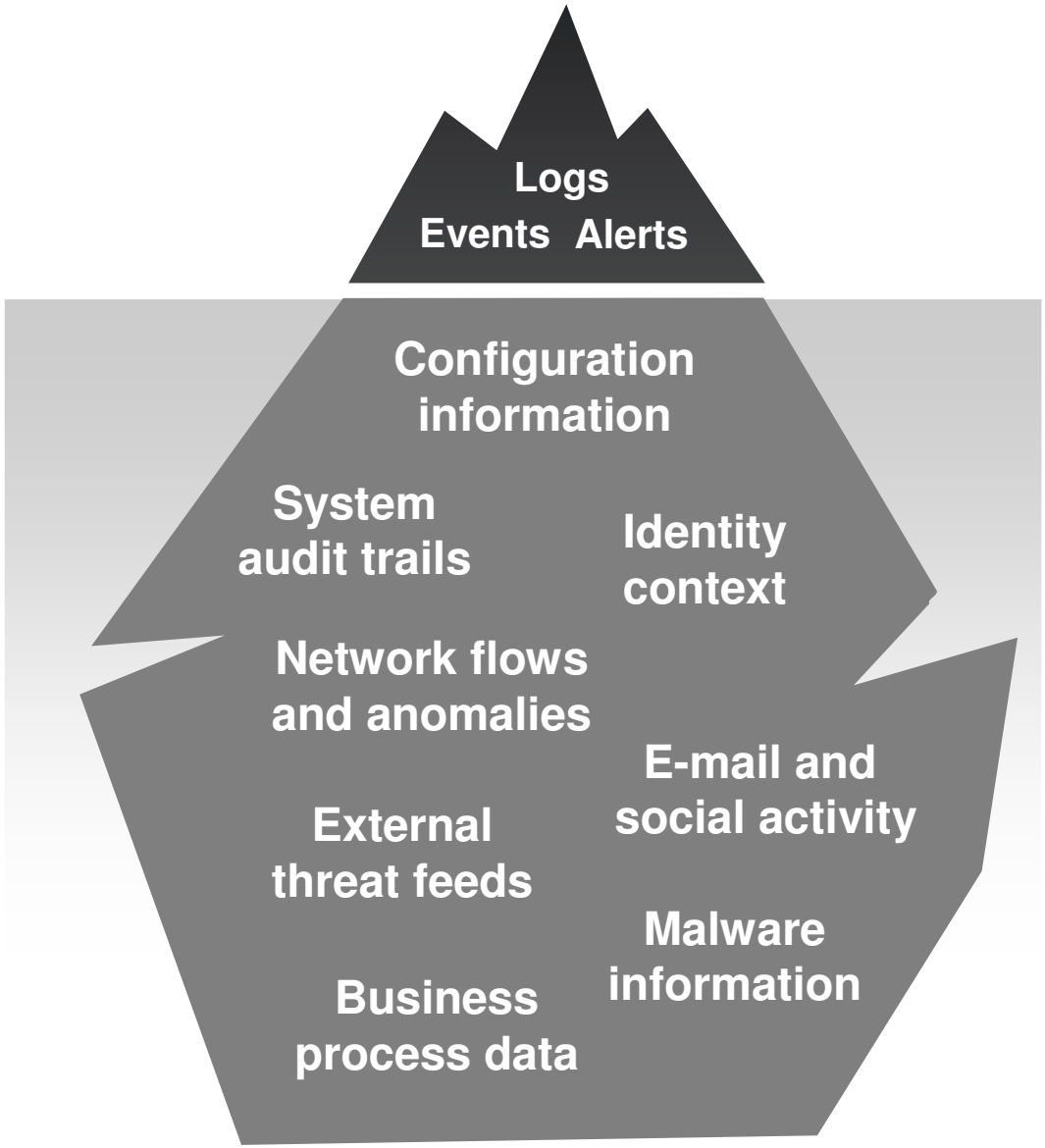
Then: Reaction

- Read about the latest threats from blogs and news
- Match against known signatures and bad actors

Now: Situational Awareness

- Consume real-time intelligence about the latest threats
- Correlate alerts against external behavior and reputation
- Proactively block bad domains, IP address and malware

Security Intelligence



Then: Collection

- Log collection
- Signature-based detection

Now: Intelligence

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics

Customer Challenges

Detecting threats
- Arm yourself with comprehensive security intelligence

Consolidating data silos
- Collect, correlate and report on data in one integrated solution

Detecting insider fraud
- Next-generation SIEM with identity correlation

Better predicting risks to your business
- Full life cycle of compliance and risk management for network and security infrastructures

Addressing regulation mandates
- Automated data collection and configuration audits

IBM designs security into systems for comprehensive protection and Security Ready IT infrastructure

A comprehensive security approach in our systems design…

Security Built-In	**Not an afterthought, secure out of the box**
Design for Accountability	All security-relevant actions are logged and audited
Design for Regulations	Flexible support for the constraints set by regulators
Design for Privacy	Enables the principles of notice, choice and access
Multiple Levels of Protection	Defense in depth is a general principle for detection

…leads to comprehensive protection for all layers of the stack

IBM

Applications	Define granular software policies to run across the entire data center
Operating System	Trusted Execution ensure only software can load and execute
Hypervisor	Security chain of trust built into the hardware
Firmware	Firmware ensures only IBM-signed hypervisors can install and load
Hardware	Microprocessor based chip security

End-to-End Security Coverage with IBM Systems… like **System z**

How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the mainframe?

How do you know your private customer data is encrypted with key mgmt?

Is your mainframe security configured properly?

Where can your DB2 or IMS auditors get at the information they need?

Can you prove that all critical data is backed up and recoverable?

Do you know if administrators are abusing privileges?

How do you know only authorized users are given user accounts?

How did you protect your Web services applications?

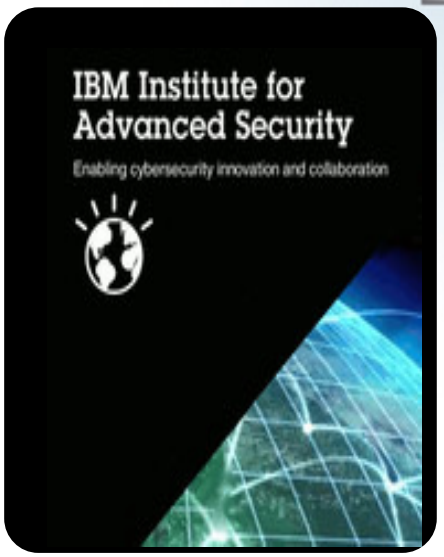
RACF	z/OS Communications Server IBM Security NIPS	Guardium and Optim Solutions IBM Security Key Lifecycle Manager	Security zSecure suite	DB2 and IMS Audit Management Expert	Tivoli zStorage	QRadar SIEM zSecure Compliance and Auditing	Identity Manager Access Manager	Tivoli Federated Identity Mgr

Platform Infrastructure ⟷ **Data Privacy** ⟷ **Compliance and Audit** ⟷ **Extended Enterprise**

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

IBM Expertise: *Unmatched global coverage and security awareness*

Zurich, CH
Waltham, US
Fredericton, CA
Delft, NL
Belfast, N IR
Ottawa, CA
Toronto, CA
Brussels, BE
IAS Europe
Herzliya, IL
Boulder, US
Almaden, US
TJ Watson, US
Tokyo, JP
IAS Americas
Detroit, US
Bangalore, IN
Haifa, IL
Costa Mesa, US
Tokyo, JP
Raleigh, US
Austin, US
Atlanta, US
Pune, IN
Taipei, TW
Atlanta, US
Atlanta, US
Bangalore, IN
Singapore, SG
Brisbane, AU
New Delhi, IN
Gold Coast, AU
Hortolândia, BR
Perth, AU



- Security Operations Centers
- Security Research Centers
- Security Solution Development Centers
- Institute for Advanced Security Branches

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