

---

Security Intelligence.  
**Think Integrated.**

# IBM Security Services

Security implications of the use of smarter and bigger data

Infosecurity Europe, April 2013

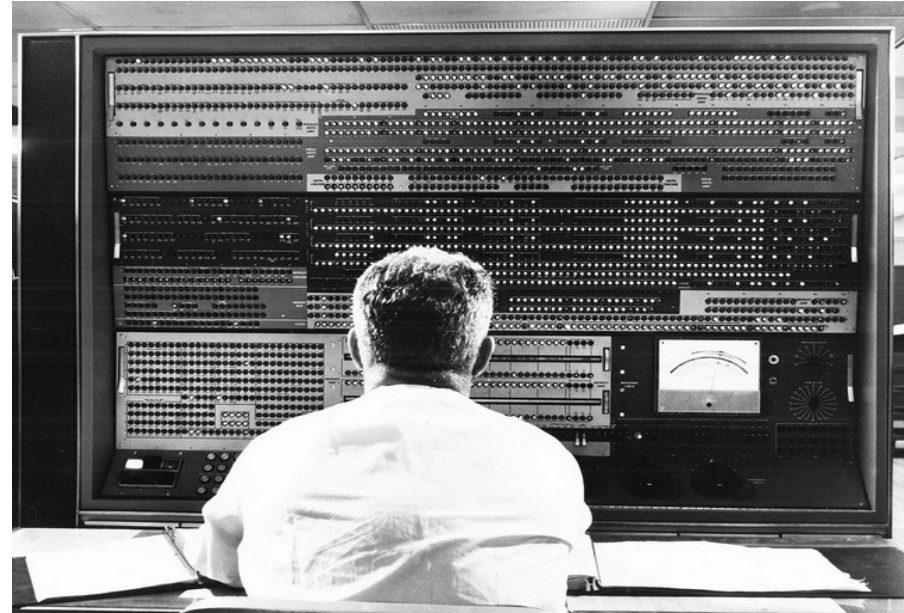


# What is Big Data?



## The Facts

- The term “Big Data” is a bit of a misnomer.
- The Definition.....
  - Big Data applies to information that can’t be processed or analysed using traditional processes or tools.
- Big Data is about the collection, storage, correlation, analysis and application of this data – unlocking it’s business value through the creation of actionable business intelligence and insights.
- 2.5 Quintillion bytes of data created every day.
- 1 Billion transistors for every person on the planet.
- 4 Billion mobile phones worldwide.
  - Growing to 10 Billion internet connected mobile devices by 2016.
- 30 Billion RFID tags.
  
- Organisations are facing the challenge of how to get more value from the rich data in their systems while also ensuring the data is secure and being handled appropriately.



# Then and Now





## IBM and Big Data.

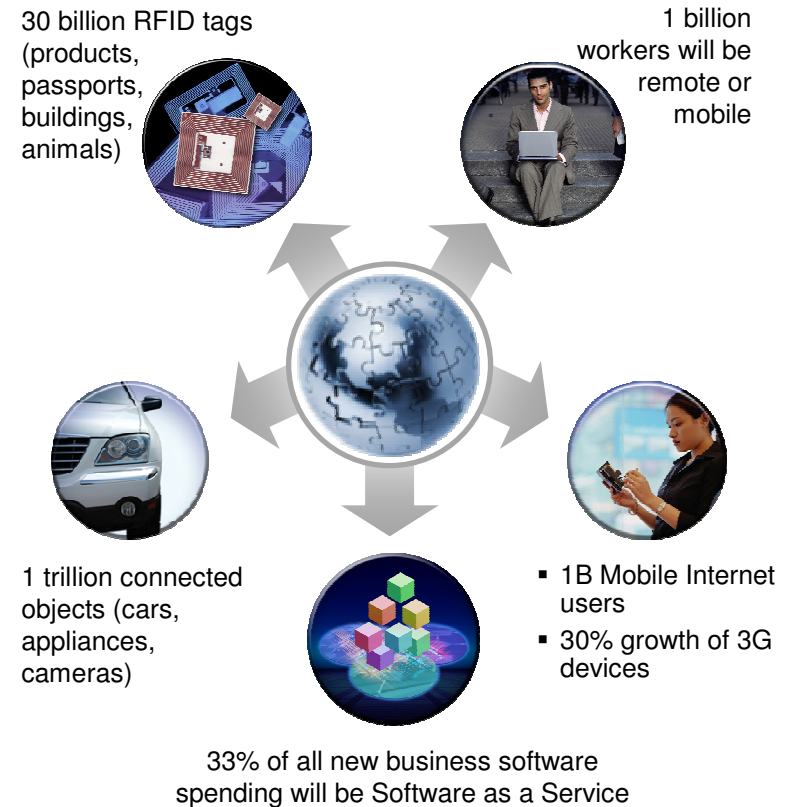
- 1956 – IBM introduce first magnetic hard disk for data storage.
  - 2000 bits at a cost of \$10,000 per megabyte. (Today is 10 cents)
- 1970 – IBM published concept of relational databases.
- 1971 – IBM built first operational speech recognition application.
- 1980 – IBM built first prototype computer using RISC architecture.
- 1993 – Scalable Parallel Systems.
- 1997 – Deep Blue.
- 2009 – First Nationwide Smart Energy and Water Grid.
- 2011 – Watson.

As organisations embrace new technologies, adopt new business models and becoming more interconnected, their security risk is increasing

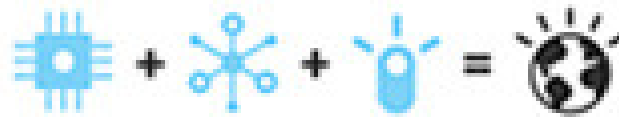
### Embracing New Technologies, Adopting New Business Models



### Exploding and Interconnected Digital Universe



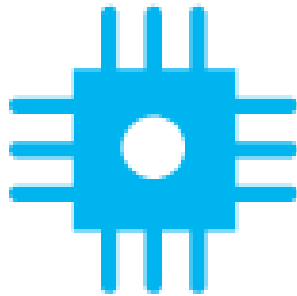
# Value of Data on a Smarter Planet



## Smarter Planet - what do we mean?

By smarter, we mean the world  
is becoming:

instrumented



+

interconnected



+

intelligent



- *Some case studies...*
- *And pause to think what if the integrity, or veracity, of data is questionable?*

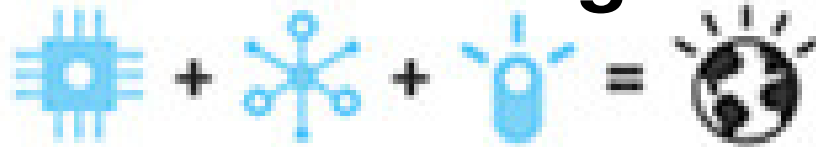








# Smarter Intelligence with Big Data



## Headlines for 2012

### IBM X-Force 2012 Trends and Risks Report Highlights *March 2013*

#### Headlines

- SQL injection remains tried and tested vector (online)
  - BYOD (without careful policy and governance) brings perils
  - Web browser exploit kits remain a popular tool
  - Java a key target in 2012; exploits to continue in 2013
  - Spam volume flat, but sophistication increasing
  - Web apps account for most disclosed vulnerabilities (53% XSS alone)
  - Social media rich source of data for targeting attacks
- 17B** analyzed web pages & images
- 40M** spam & phishing attacks / month
- 68K** documented vulnerabilities
- 15B** security events monitored daily

#### Threats

- Malware and the malicious web
- Web content trends
- Spam and phishing

#### Operational security practices

- Vulnerabilities and exploitation

#### Emerging Trends in Security

- Mobile devices more secure than traditional devices by 2014
- Separation of personas or roles

# Extending Security Intelligence with Big Data

## Advanced Security Analytics & Correlation Engine

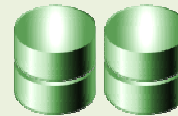
### Data Sources

- Security Devices
- Server and Host Logs
- Network and Virtual Activity
- Database Activity
- Application Activity
- Vulnerability and Config Data
- Threat Intelligence Feeds
- User Activity and Behavior
- Web, Blogs, & Social Activity
- Business Transactions
- Unstructured data (e.g. Email)



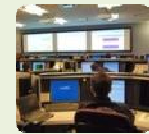
### Real-time Processing

- Focus on HOT, real-time data
- Event normalization
- Real-time correlation
- Data enrichment



### Security Operations

- Detailed security metrics
- Activity & event graphs
- Incident management
- Compliance reporting



## Big Data Security Workbench

### Big Data Warehouse

- Storage for HOT, Warm & cold data
- Unstructured and structured
- Distributed infrastructure
- Preserves raw data
- Scalable platform
- Large-scale machine learning
- Hadoop-based backend



### Big Data Analytics and Forensics

- Advanced visuals and interaction
- Predictive and decision modeling
- Ad hoc and historical queries
- Transaction and geo analysis
- Custom reports and dashboards
- Pluggable UI
- Collaborative sharing tools

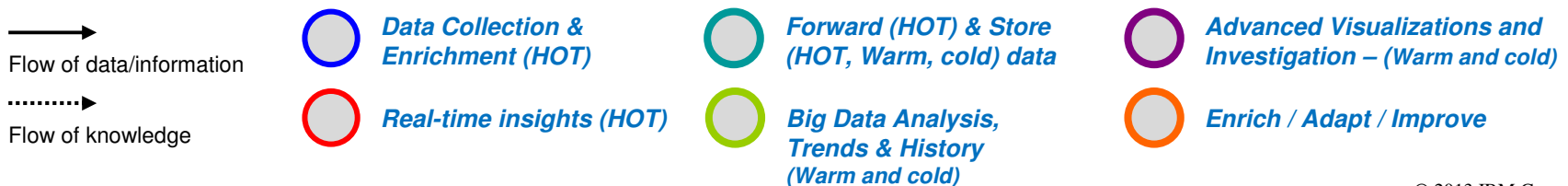
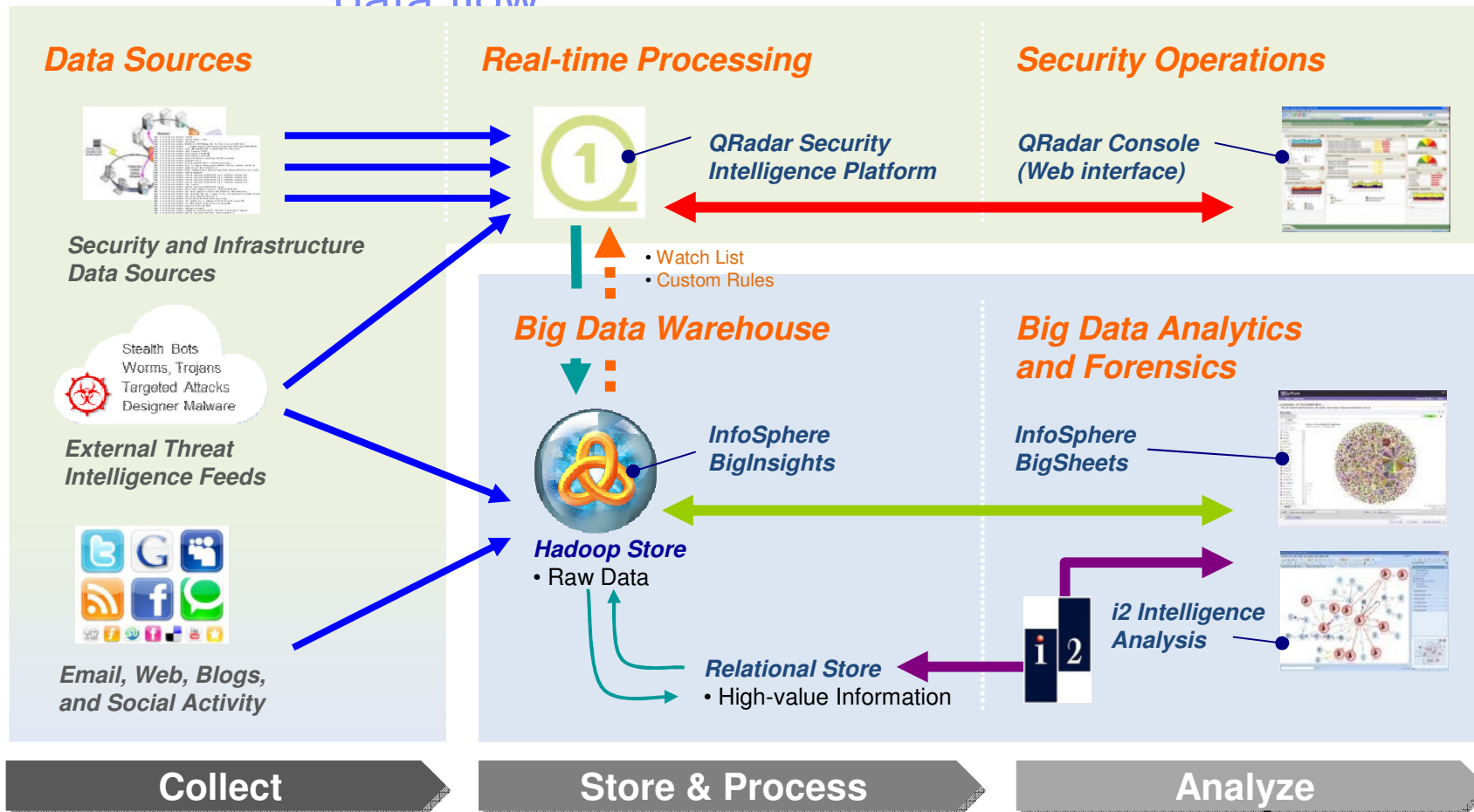


Collect

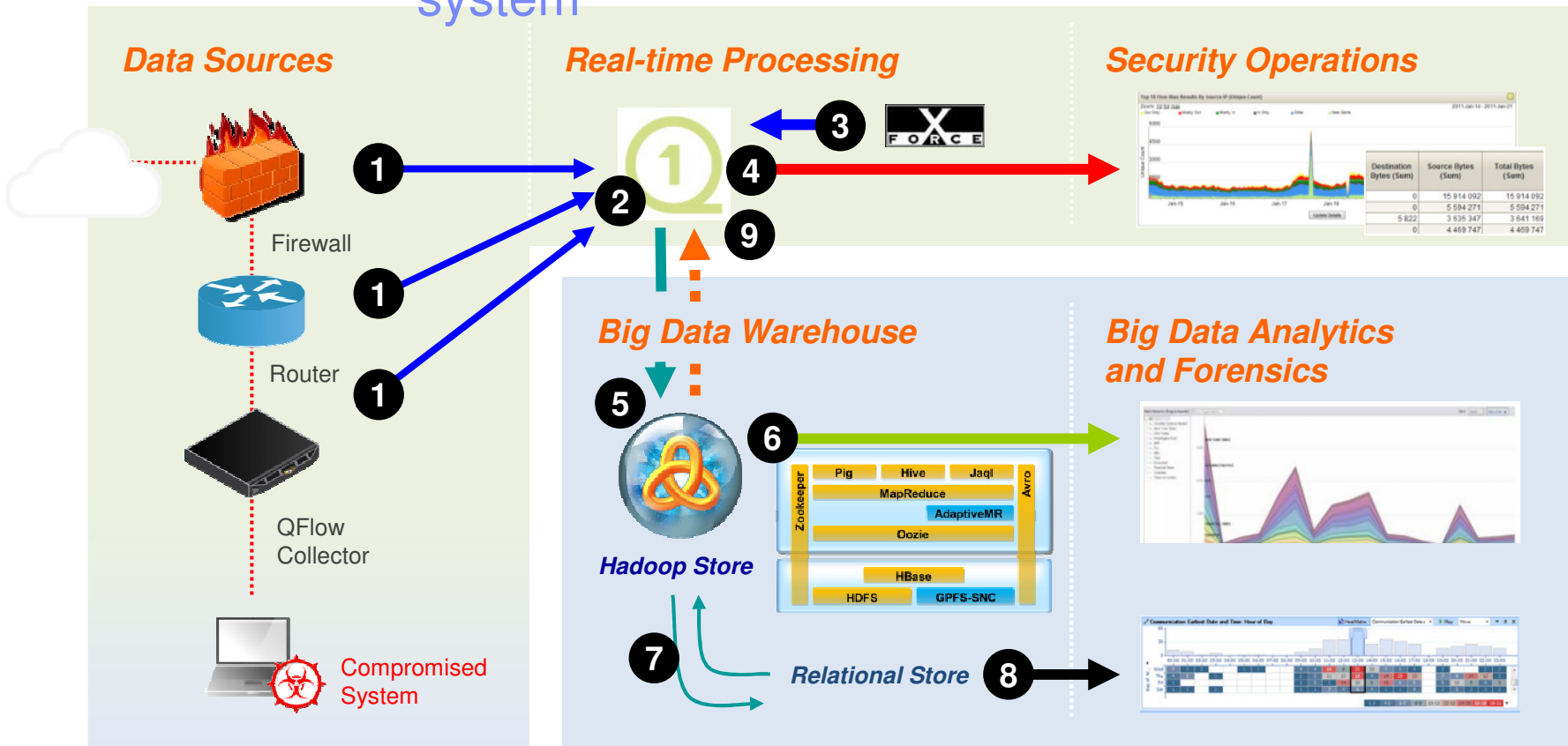
Store & Process

Analyze

# Security Intelligence with Big Data– Components and data flow



# Use case #1 – Detection of an internal compromised system



**Requirements**

Source: Netflow  
 Sample Size: >100GB /src  
 Query time: <30sec  
 Analytics: Time interval and network flow size

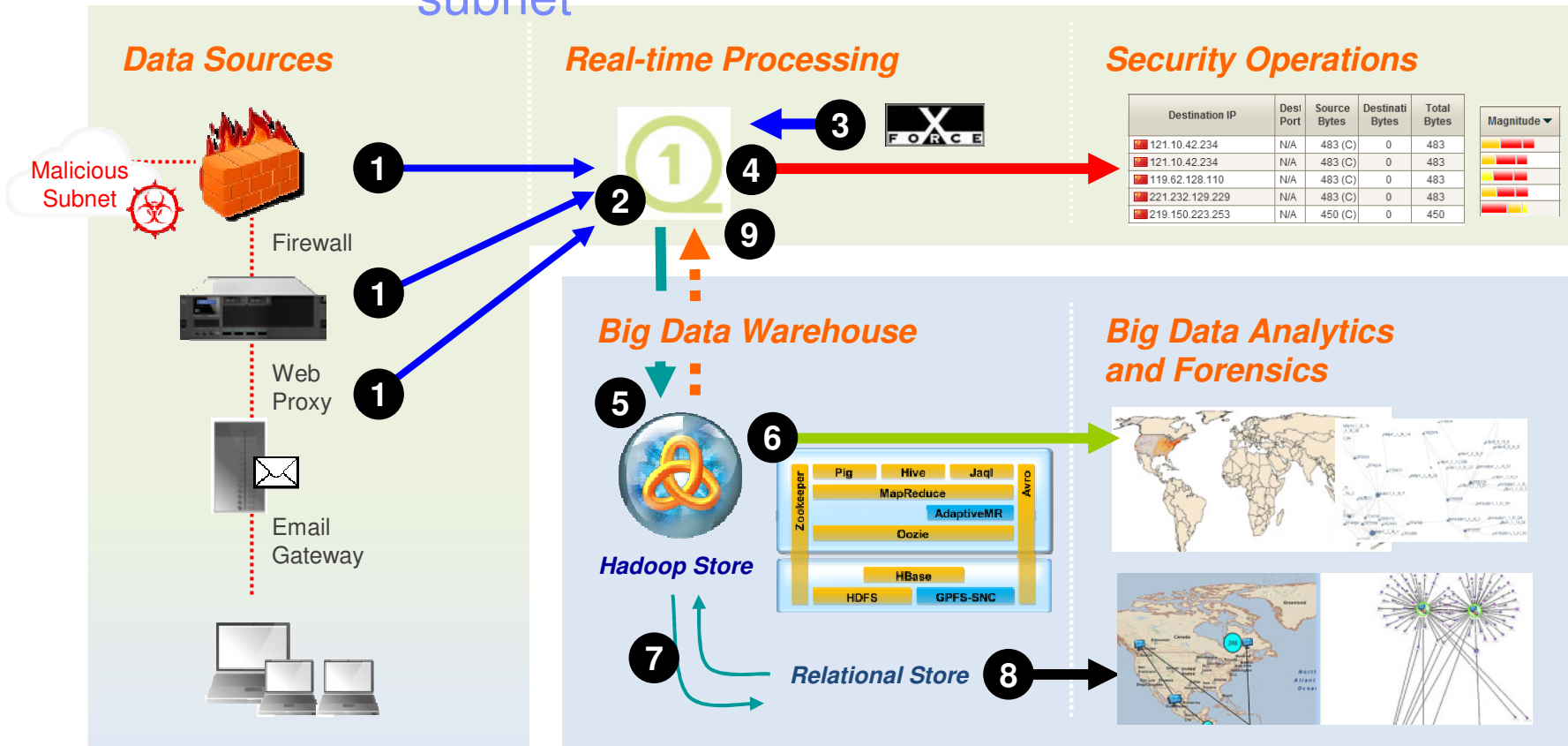
**IBM Approach**

1. Netflow extracted, sent to QRadar
2. Bi-directional flow processing
3. Correlation against external threats
4. Real-time flow analysis to the SOC

5. Enriched flows sent to BigInsights
6. Custom BigSheets queries / analytics
7. Post-processed data storage
8. i2 time-based visuals / analytics
9. Update of QRadar real-time rule sets



## Use case #2 – Detection of a malicious external subnet



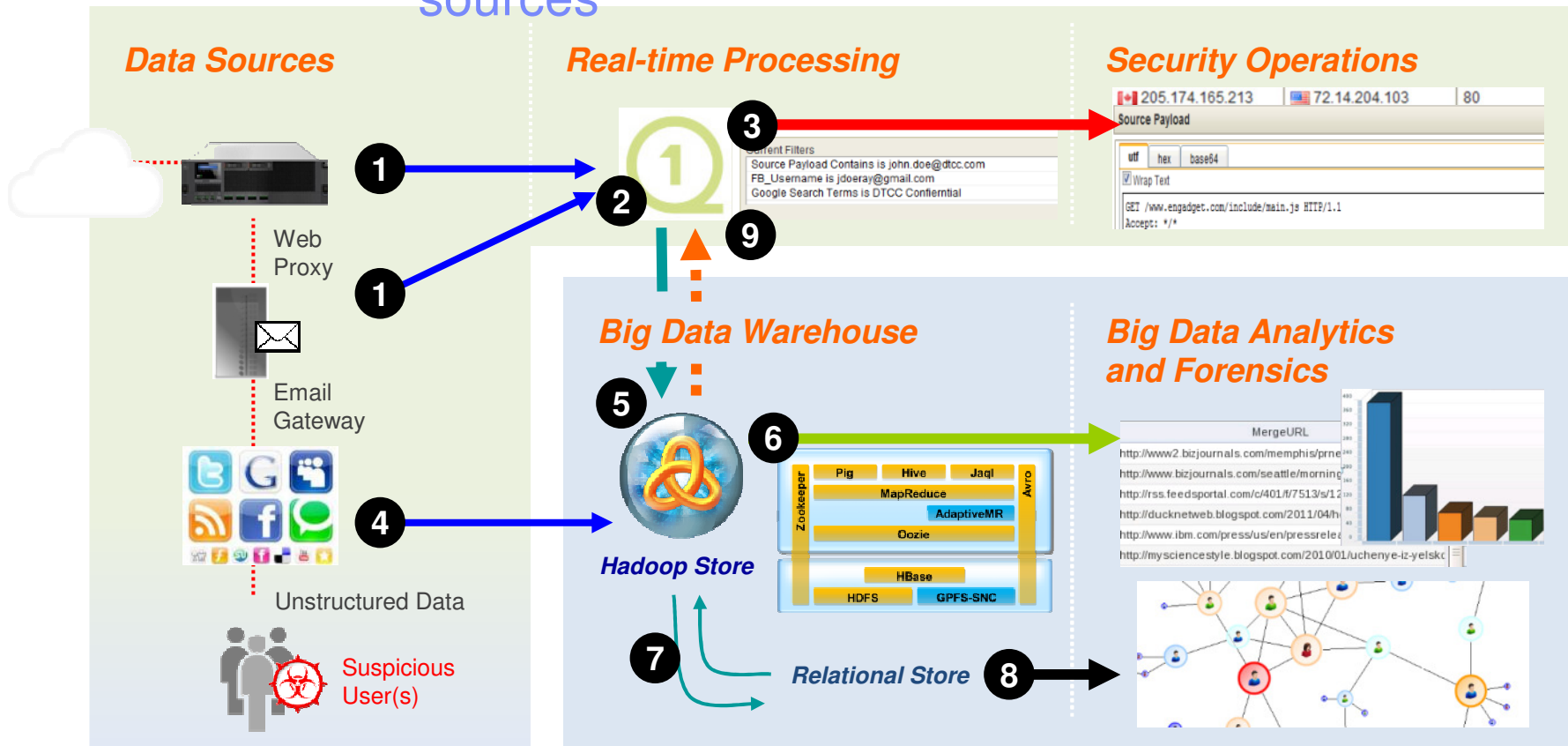
### Requirements

Source: FW, email, proxy  
 Sample Size: >30GB /src  
 Query time: <30sec  
 Analytics: Graphical view of malicious subnet

### IBM Approach

1. Logs extracted, sent to QRadar
2. Event normalization
3. Correlation against external threats
4. Real-time IP / subnet alerts to SOC
5. Log / event forwarding to BigInsights
6. Custom BigSheets queries / analytics
7. Post-processed data storage
8. i2 geo and network visuals / analytics
9. Update of QRadar real-time rule sets

## Use case #3 – User profiling based on multiple sources



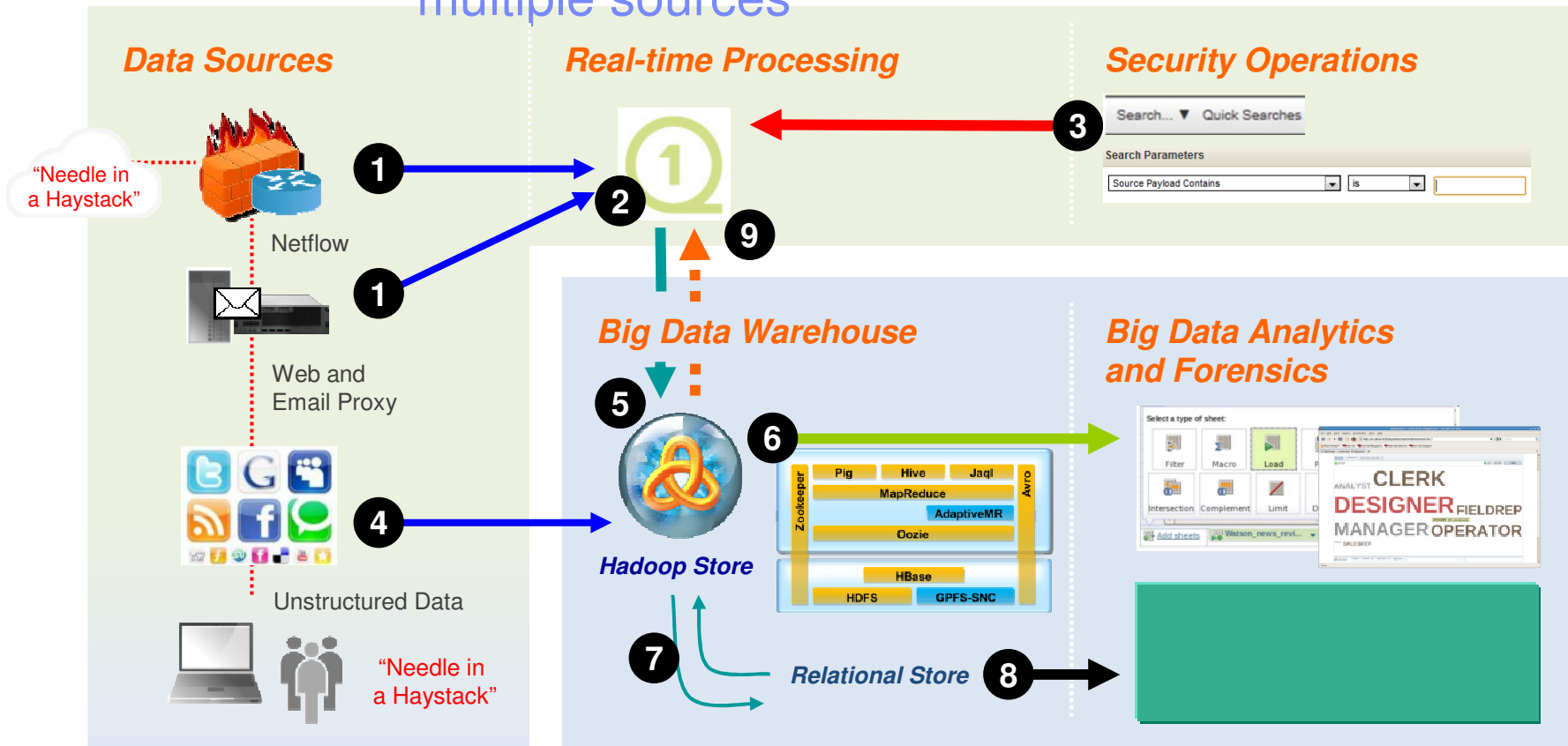
### Requirements

Source: proxy, email, unstructured text  
 Sample Size: >25GB /src  
 Query time: <45sec  
 Analytics: Multiple

### IBM Approach

1. Logs extracted, sent to QRadar
2. Event normalization
3. Custom filtered events sent to SOC
4. Unstructured data to BigInsights
5. Log / event forwarding to BigInsights
6. Custom BigSheets queries / analytics
7. Post-processed data storage
8. i2 link-based visuals / analytics
9. Update of QRadar real-time rule sets

## Use case #4 – Ad hoc query for specific data on multiple sources



### Requirements

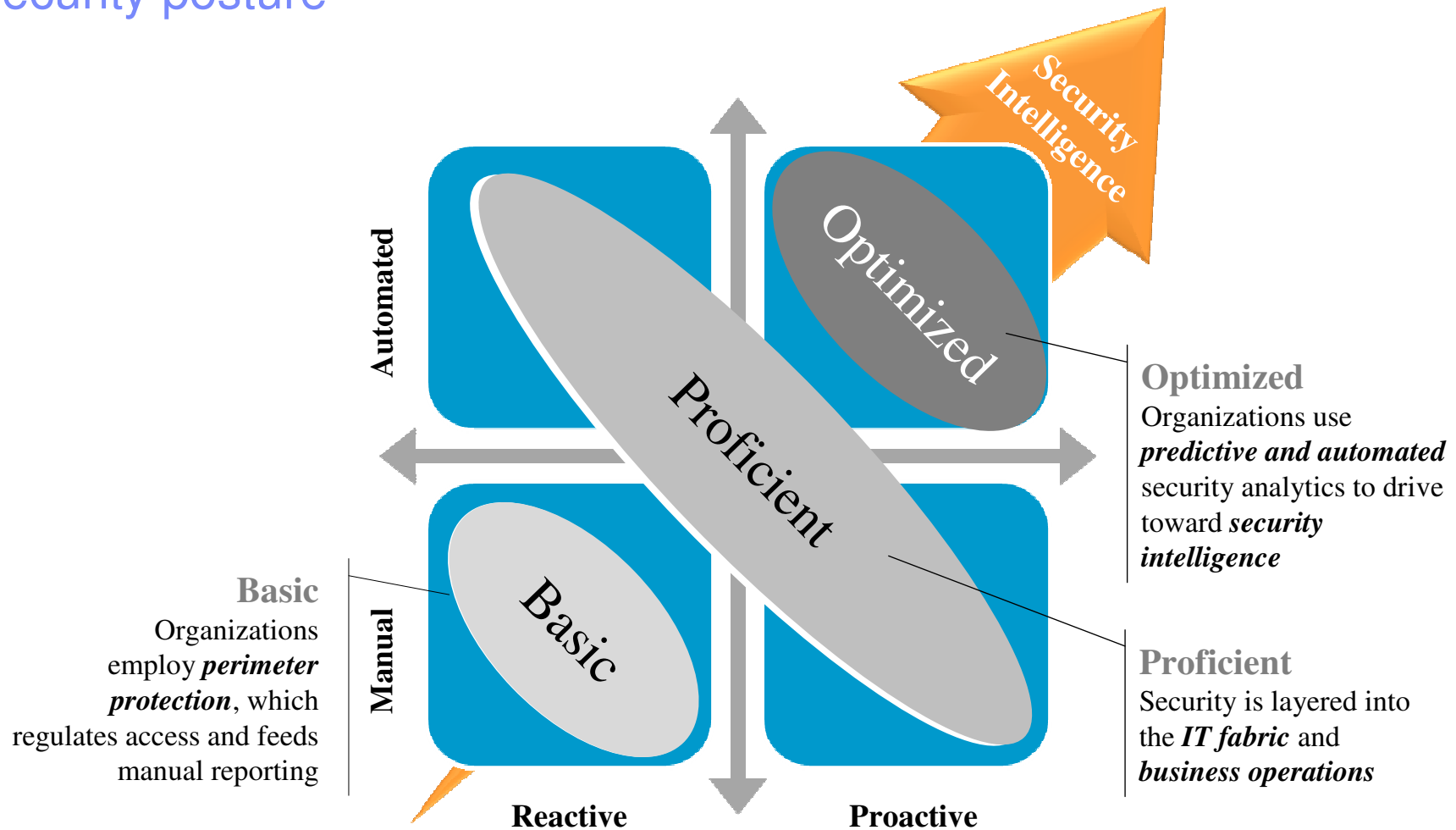
Source: All  
 Sample Size: >20GB /src  
 Query time: <45sec  
 Analytics: Search for IP, FQDN and/or email address

### IBM Approach

1. Netflow and logs sent to QRadar
2. Event and flow processing
3. Ad hoc payload search from SOC
4. Unstructured data to BigInsights

5. Events and flows sent to BigInsights
6. Custom BigSheets queries / analytics
7. Post-processed data storage
8. i2 text-based, federated search
9. Update of QRadar real-time rule sets

# In this “new normal”, organisations need an intelligent view of their security posture





**Let us not forget the Security challenges of using Big Data**

## So what must we consider?

- **As always...**

- Availability, Integrity and Confidentiality
- Data at rest and in transit. but also...
  - At point of creation.. a Trillion ‘smart’ devices...but can they be accurately identified, trusted. and...
  - At point of consumption; who uses the ‘intelligence’ and where – how is it accessed

- **Risk increased by**

- collaborative nature of data collection/data sourcing and storage – across intra and inter business **boundaries** and multiple systems/technologies;
- tooling – especially Open Source software such as Hadoop
- use of intelligent search engines – no longer possible to rely on ‘needle in haystack’/’security by obscurity’ defence
- Greater risk further down the supply chain.

## So what must we consider? (continued)

- **Data Privacy and Data Protection**

- A data subject has the right by notice, to prevent a data controller from taking evaluation decisions concerning him or her by automated means alone.
- Data controller must be able to explain the logic.

- **Data Inference**

- What can you infer from data processing it in more intelligent ways.
- Remember how fraud engines work.

- **The aggregation of data**

- Data has value, but the value varies depending on the nature of the business.
- Current/future market value of personal data...

- **Your supply chain**

- Are you and all your suppliers on the same page when it comes to Information Security?


# IBM developed 10 essential practices to better security intelligence

## Essential practices




1. Build a risk-aware culture and management system

6. Control network access and help assure resilience

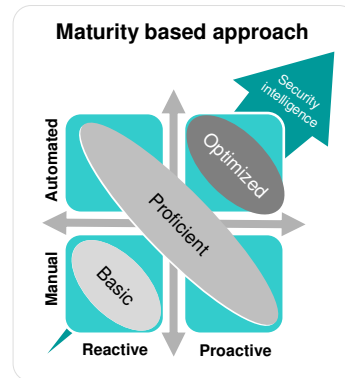



2. Manage security incidents with greater intelligence

7. Address new complexity of cloud and virtualisation




3. Defend the mobile and social workplace




8. Manage third-party security compliance





4. Security-rich services, by design

9. Better secure data and protect privacy

5. Automate security 'hygiene'

10. Manage the identity lifecycle





## IT Trends for 2013

- **Cloud security** will move from hype to a mature solution and will move on.
- **Advances in BYOD/mobile security** will improve and be more secure than laptops by 2014
  - Brings a new threat actor
- **Compliance will be a big driver in 2013.** In Europe and the UK change in DPA legislation
  - Fines up to 2% of annual turnover
  - Changing of boundaries of controller / processor
  - Mandatory for all organisation to have data privacy officers
- **Data explosion will increase.**
  - Type of data collected and inspected to detect advanced threats will explode
  - As the security perimeter evolves so will the types of threats, thus creating the need for greater analysis
  - IBM Q1 labs plus X-Force will be at the front of this

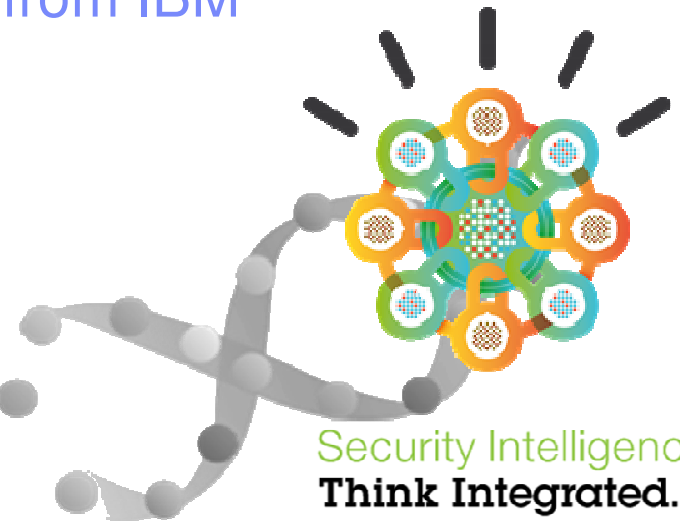
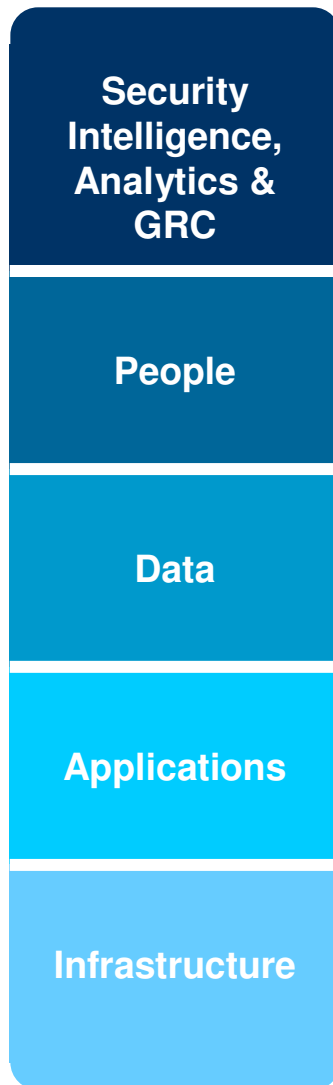
## Threats to consider in 2013

- **Cyber-(in)security:** Increased government presence in cyberspace will have a profound impact on the future of information security.
- **Supply chain security:** More organisations will fall victim to information security incidents at their suppliers.
- **Big data:** As big data continues to become a game-changer for businesses, the security risks have become even greater.
- **Data security in the cloud:** The rising costs that are associated with proving cloud computing compliance and external attacks on the cloud will increase in 2013.
- **Consumerisation:** securing consumer devices. If implemented poorly, a personal device strategy in the workplace could facilitate accidental disclosures due to loss of boundary between work and personal data and more business information being held in unprotected manner on consumer devices.

## At the end of the day

- **“Big Data”** is no different from any other form of data we handle on a day to day basis.
  - It has value.
  - It has rules governing its use.
  
- **Information Security** is not rocket science.
  
- **Get the basics right:**
  - Embed the culture of security in the organisation.
  - Awareness and training.
  - “Secure by Design”
  
- **Information Security** has always been and will always be an enabler for business.

## Integrated security thinking from IBM



● **Brendan Byrne**

Associate Partner, Consulting and SI Leader for IBM Security Services

E-mail: [bbyrne@uk.ibm.com](mailto:bbyrne@uk.ibm.com)

Mobile: +44(0) 776 428 3054

**Adrian Harris**

Information Security Architect and CLAS Consultant, IBM Security Services

E-mail: [adrian.harris@uk.ibm.com](mailto:adrian.harris@uk.ibm.com)



## Trademarks and notes

### **IBM United Kingdom Limited**

PO Box 41  
North Harbour  
Portsmouth  
Hampshire  
PO6 3AU  
United Kingdom

### **IBM Ireland Limited**

Oldbrook House  
24-32 Pembroke Road  
Dublin 4

IBM Ireland Limited is registered in Ireland under company number 16226.

The IBM home page can be found at **ibm.com**, IBM, the IBM logo, ibm.com and IBM X-FORCE 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**

Other company, product and service names may be trademarks, or service marks of others.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program or service is not intended to imply that only IBM products, programs or services may be used. Any functionally equivalent product, program or service may be used instead.

This publication is for general guidance only.

Information is subject to change without notice. Please contact your local IBM sales office or reseller for latest information on IBM products and services.

IBM does not provide legal, accounting or audit advice or represent or warrant that its products or services ensure compliance with laws. Clients are responsible for compliance with applicable securities laws and regulations, including national laws and regulations.

Photographs may show design models.

© Copyright IBM Corporation 2013