

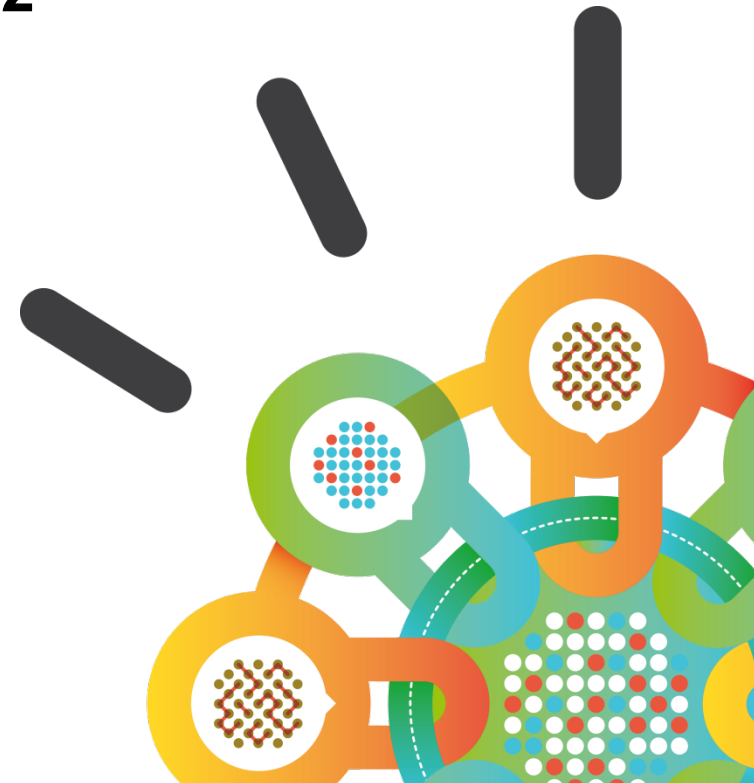
IBM Security

# Emerging Threats in 2012

IBM South Bank – 26<sup>th</sup> September 2012

*Peter Jopling*  
*joplingp@uk.ibm.com*

*Solutions Manager- SEi Practice UK – WW Security Tiger Team*  
*IBM Security Systems Division*





**ALERTCON 1**

# The Planet Is Getting More...

**Smart Supply Chains**



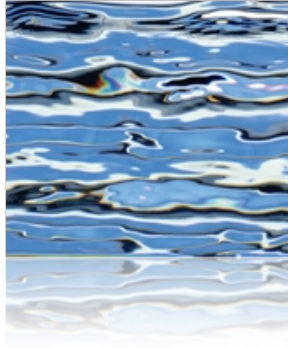
**Smart Countries**



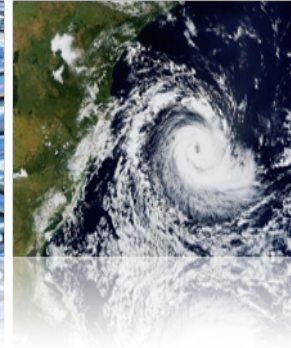
**Smart Retail**



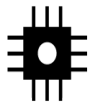
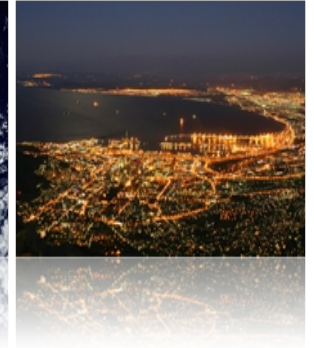
**Smart Water Management**



**Smart Weather**



**Smart Energy Grids**



**INSTRUMENTED**



**INTERCONNECTED**

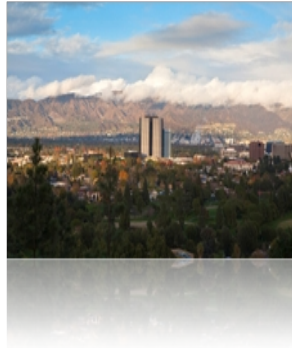


**INTELLIGENT**

**Smart Oil Field Technologies**



**Smart Regions**



**Smart Healthcare**



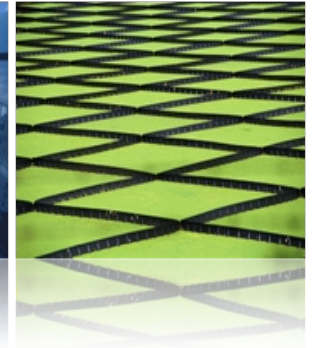
**Smart Traffic Systems**



**Smart Cities**



**Smart Food Systems**





ALERTCON 1

# Explosion of data:

Harness **big data** to gain insight and develop new offerings

**1.8**

trillion gigabytes of data added to the digital universe in 2011.<sup>1</sup>

**40%**

expected compound annual growth rate (CAGR) in the big data marketplace by 2015.<sup>2</sup>

**2 days**

The amount of data generated between the dawn of civilization and 2003 is now created every two days.<sup>3</sup>

<sup>1</sup> IDC, *The 2011 IDC Digital Universe Study Sponsored by EMC*, 2011, <http://www.emc.com/collateral/about/news/idc-emc-digital-universe-2011-infographic.pdf>

<sup>2</sup> IDC, "IDC Releases First Worldwide Big Data Technology and Services Market Forecast, Shows Big Data as the Next Essential Capability and a Foundation for the Intelligent Economy," news release, March 7, 2012, <http://www.idc.com/getdoc.jsp?containerId=prUS23355112>

<sup>3</sup> ReadWriteWeb, "Google CEO Schmidt: 'People Aren't Ready for the Technology Revolution'" Marshall Kirkpatrick, August 4, 2010; [http://www.readwriteweb.com/archives/google\\_ceo\\_schmidt\\_people\\_arent\\_ready\\_for\\_the\\_tech.php](http://www.readwriteweb.com/archives/google_ceo_schmidt_people_arent_ready_for_the_tech.php)



# Chief executive officers are under increasing pressure to deliver transformative business value—with limited resources available

Mobile in the enterprise

**90%**

of organizations will support corporate apps on a personal devices by 2014<sup>6</sup>

Innovation in the cloud

**60%**

of chief information officers view cloud computing as critical to their plans<sup>5</sup>

Increased risk

**40%**

of Fortune 500 and popular web sites contain a vulnerability<sup>2</sup>

Budgetary constraints

**71%**

of the average IT budget is dedicated to ongoing operations<sup>4</sup>

Social business

**74%**

of enterprises use social media today to communicate with clients<sup>7</sup>

Exploding data growth

**2.7ZB**

of digital content in 2012, a 50% increase from 2011<sup>3</sup>

Aging Infrastructure

**71%**

of data centers are over 7 years old<sup>1</sup>



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




ALERTCON 1

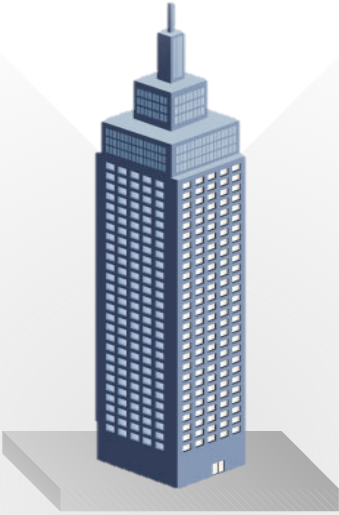
# Security trends in 2012

## Advanced Threats

Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence



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



**Enterprise Customers**

## Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed



## Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility



## Regulation and Compliance

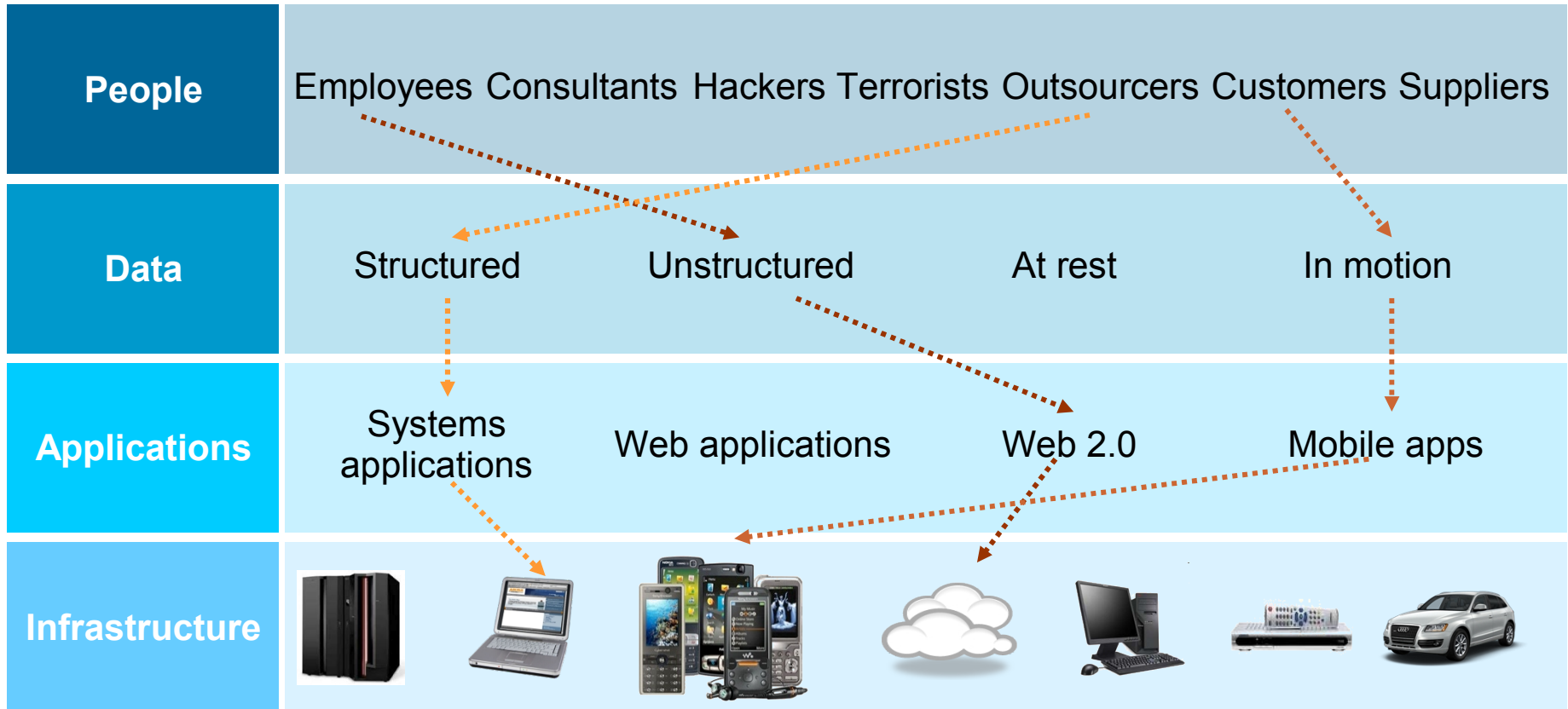
Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures





ALERTCON 1

# Solving a security issue is a complex, multi-dimensional puzzle



It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise



# IT Security is a board room discussion

ALERTCON 1

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



# Expertise: Global coverage and security awareness

ALERTCON 1



### X-Force Research

- 10B analyzed Web pages & images
- 150M intrusion attempts daily
- 40M spam & phishing attacks
- 46K documented vulnerabilities
- Millions of unique malware samples

### World Wide Managed Security Services

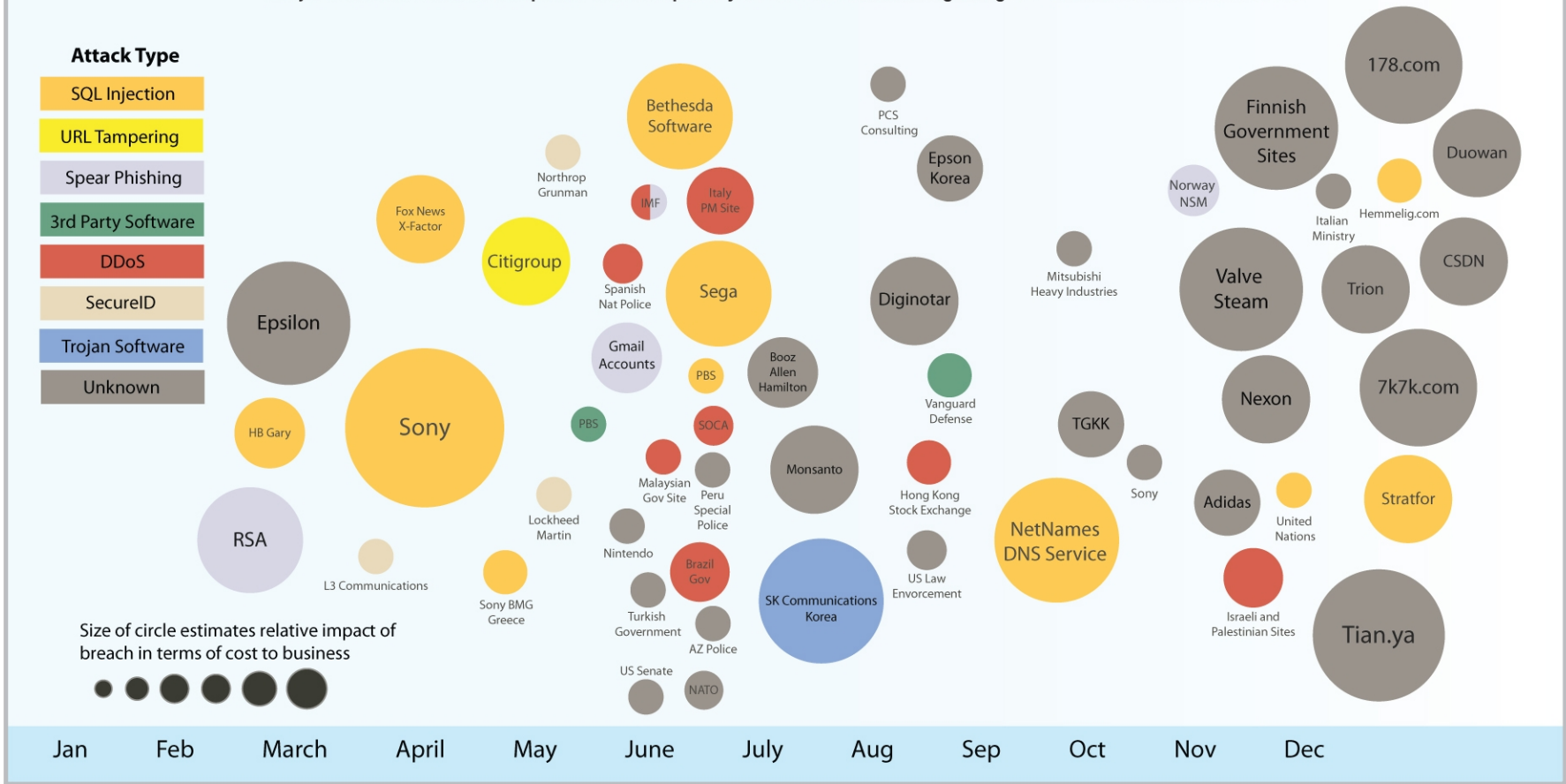
- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 15B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)





# 2011 Sampling of Security Incidents by Attack Type, Time and Impact

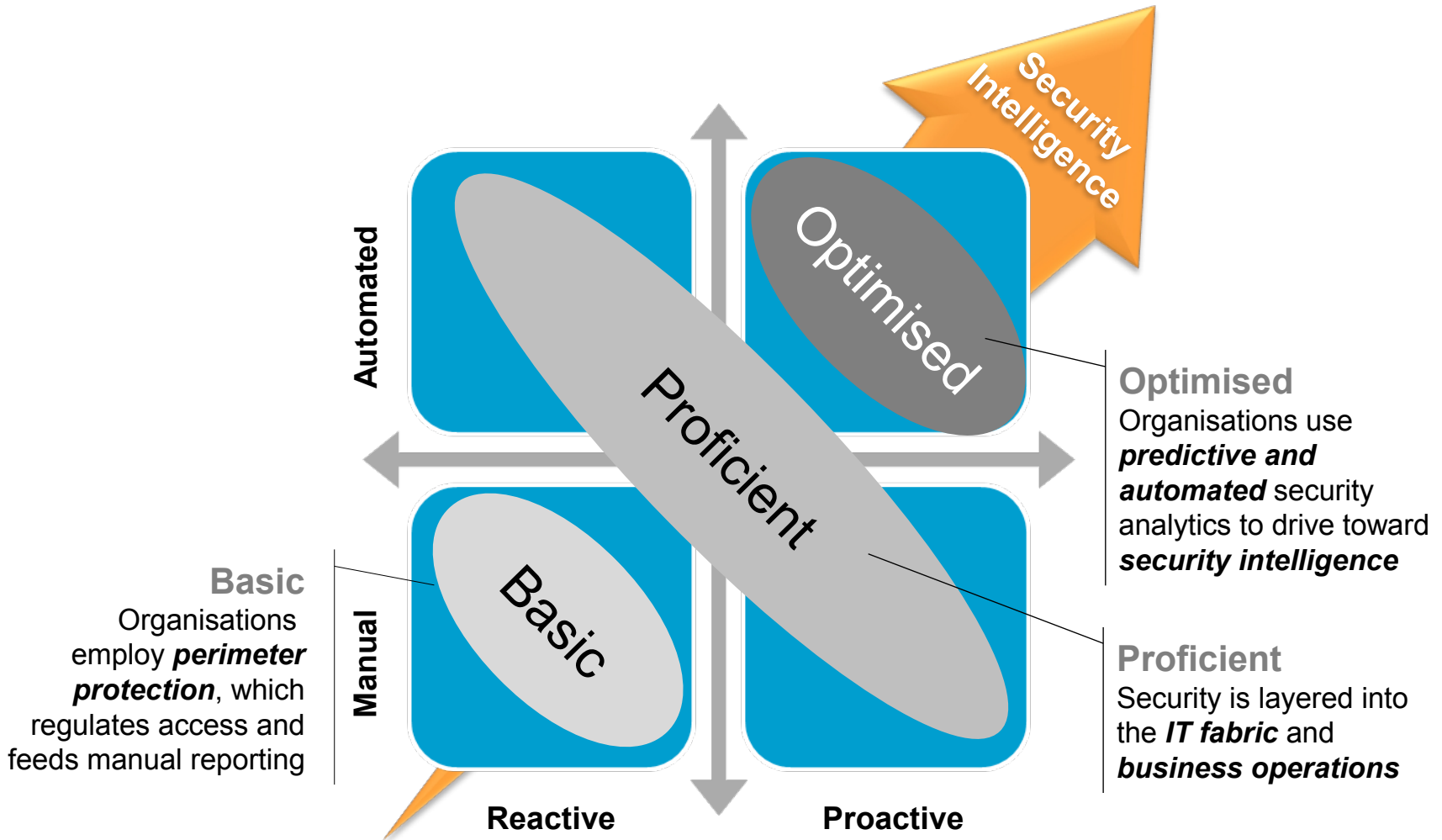
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



Source: IBM X-Force® Research and Development



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





**ALERTCON 1**

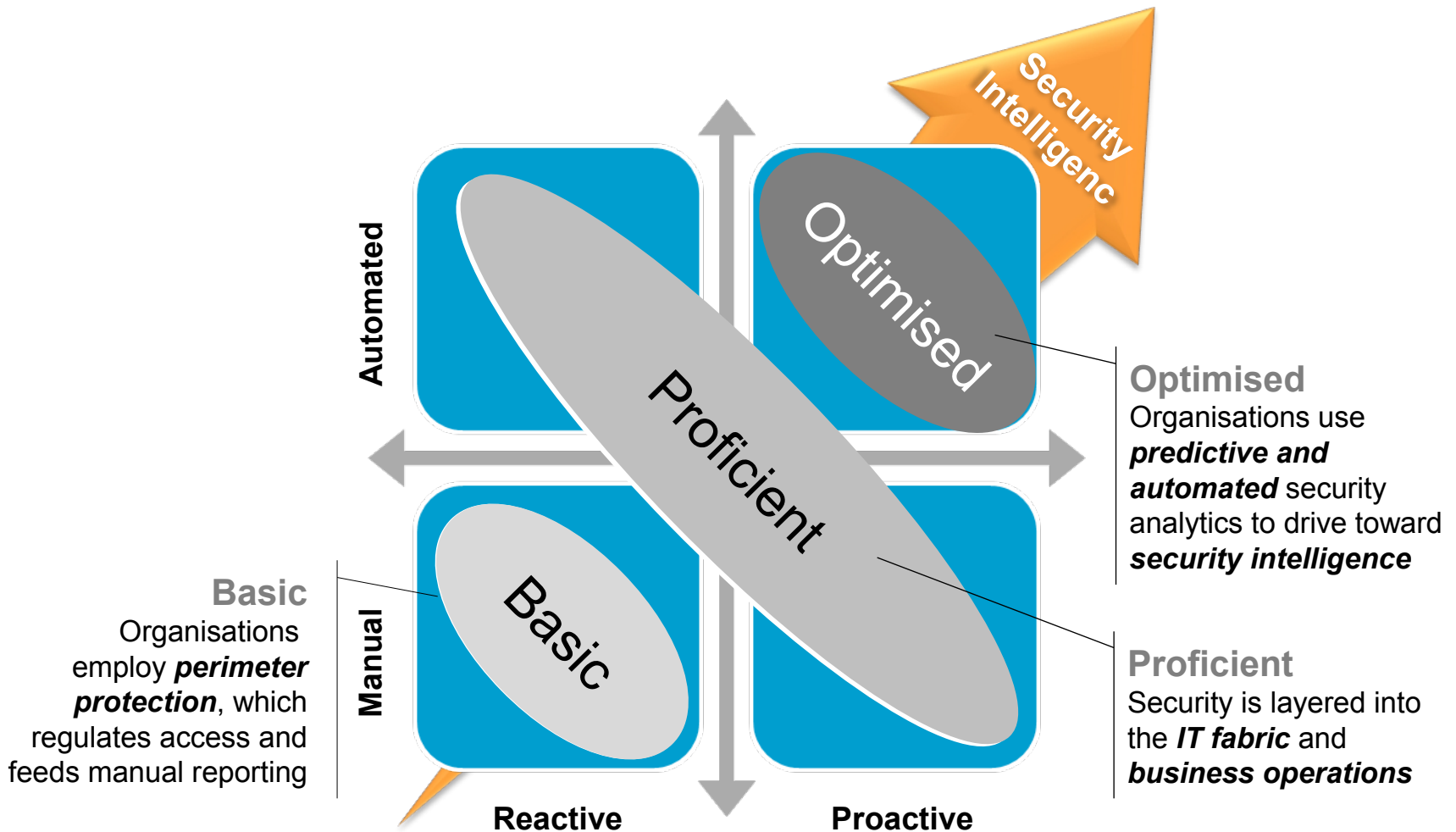
---

# Wrap up & Introduction to IBM Security Systems





In this “new normal” businesses need an intelligent view of their security posture





# X Force – Sept 2012

## IBM X-Force 2012 Mid-year Trend and Risk Report

September 2012



ALERTCON 1

- In the first half of 2012, we reported just over **4,400** new security vulnerabilities
- Since the last report, we have seen **steady growth in SQL injection**
- In the last few months we have seen major developments in the Mac malware world including the Flashback outbreak and the discovery of advanced persistent threat (APT) Mac malware
- IPv6 Day was June 6th 2012, with many organisations implementing permanent IPv6 deployments.
- On July 18th, 2012, we witnessed the take down of the Grum botnet. Grum preferred clients in the USA, Vietnam, Australia, Germany, and Brazil, with these countries sending out 29.9% of the worldwide spam before the take down,
- The rate of unpatched vulnerabilities (excluding the top ten vendors) for the first half of 2012, were the highest that IBM X-Force has seen since 2008. **47% of all vulnerabilities disclosed this year remain without a remedy.**
- The state of mobile device security is growing reports of exotic mobile malware, such as TigerBot/Android. Bmaster on Android, and Zeus/ ZITMO on multiple mobile platforms
- We continue to see steady growth in SQL injection, keeping pace with the growth of cross-site scripting, and directory traversal commands such as HTTP “DotDot” commands.
- In the world of cyber threats, obfuscation is a technique to hide or to mask the sources and methods of a security relevant event. **New obfuscation methods** are constantly evolving in an attempt to evade intrusion prevention systems (IPS) and anti-virus software. IBM Security Network IPS has special detection algorithms that assist us in monitoring these techniques around the world

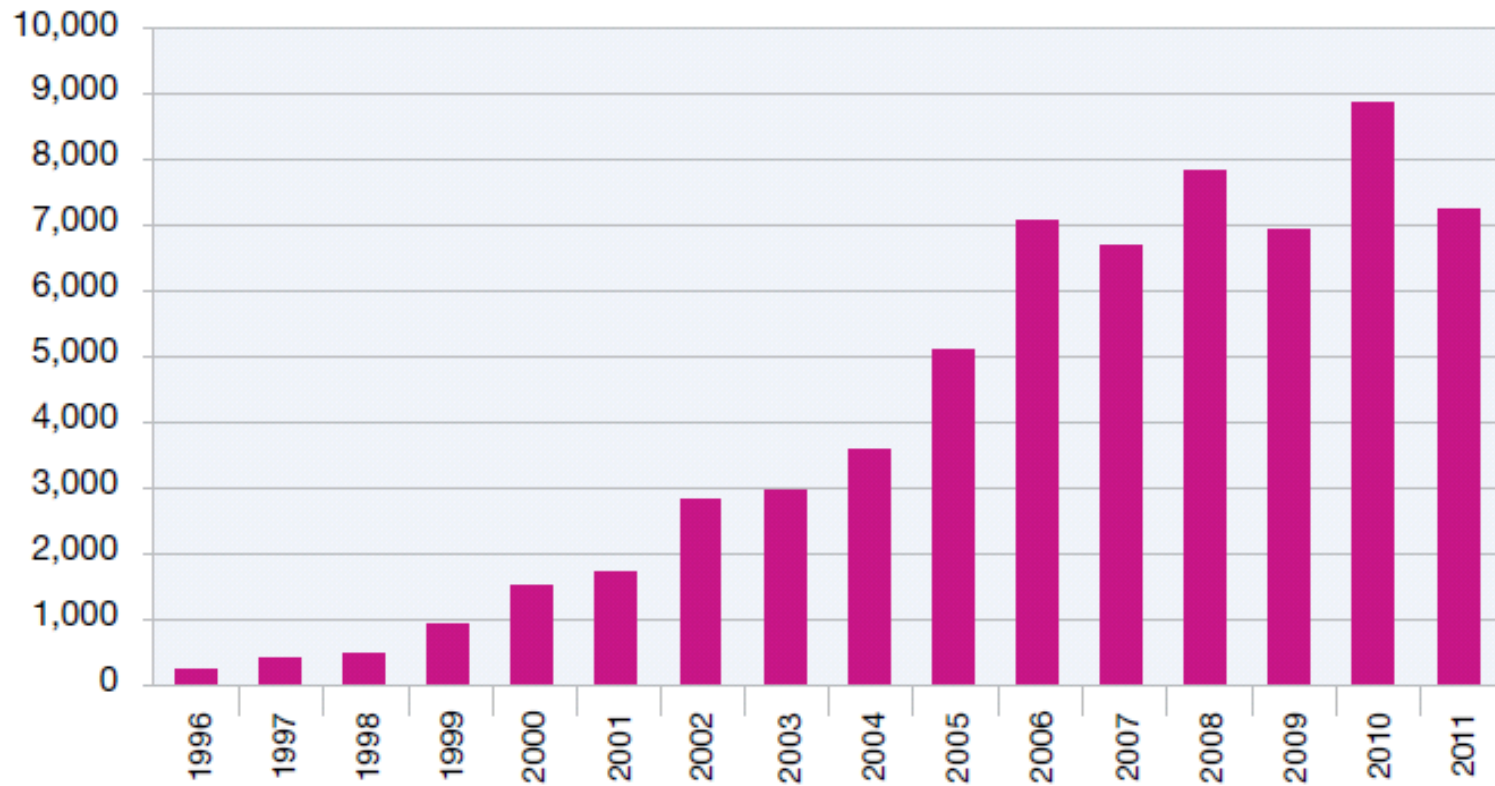
<http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF>



ALERTCON 1

61560 vulnerabilities , over 54% still unpatched by the vendor

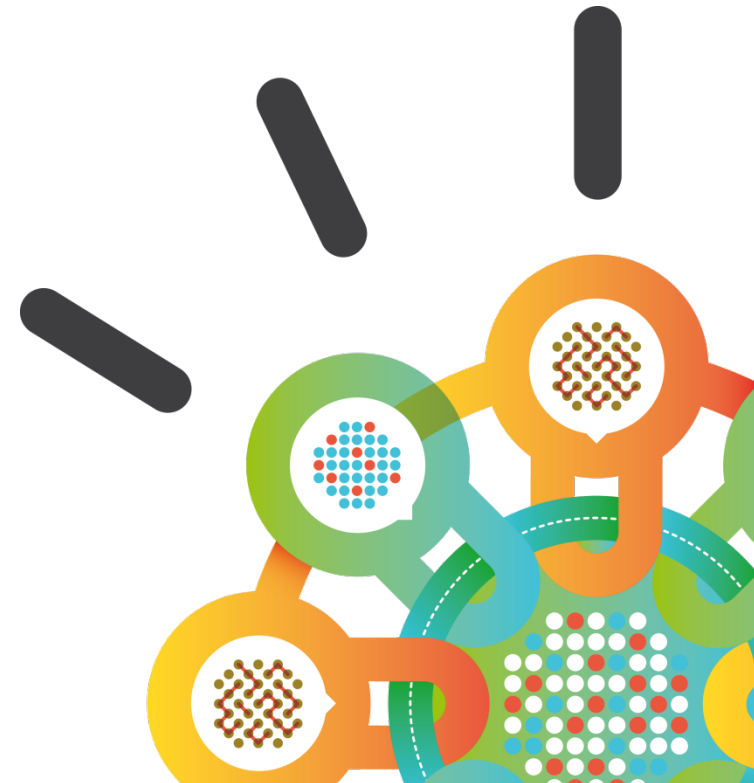
**Vulnerability Disclosures Growth by Year**  
1996-2011



X Force – March 2012

---

# IBM Security Blue Print

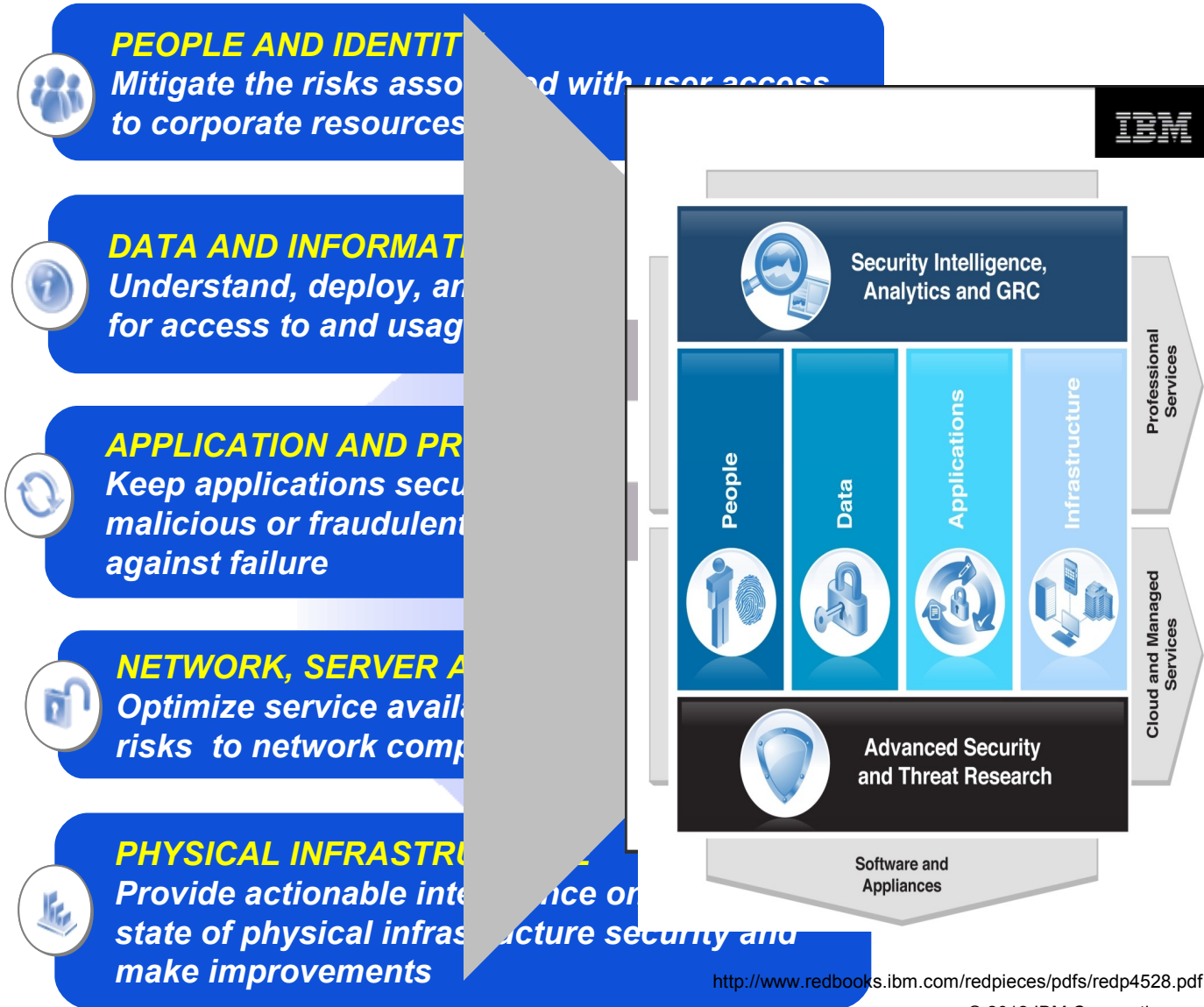






# IBM Security Blue Print

ALERTCON 1

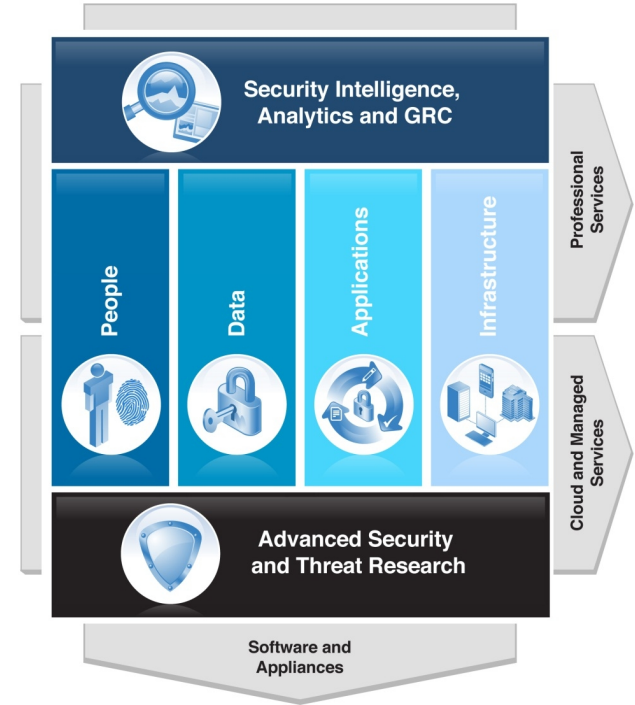




# IBM Security Systems Division

ALERTCON 1

- The **only vendor** in the market with end-to-end coverage of the security foundation
- **15,000** researchers, developers, and SMEs on security initiatives
- **3,000+** security and risk management patents
- **200+** security customer references and 50+ published case studies
- **40+** years of proven success securing the zSeries environment
- **600+** security certified employees (CISSP, CISM, CISA,..)



## Security Acquisitions:

DASCOM

consul  
an IBM company

access360  
A Better Way To  
Manage Access Rights

ENCENTUATE  
An IBM Company

watchfire

INTERNET  
SECURITY  
SYSTEMS

OUNCE LABS  
an IBM company

Guardium  
SAFEGUARDING DATABASES. AN IBM COMPANY

princeton  
softtech  
an IBM Company

Initiate

DATAPOWER

BIGFIX  
An IBM Company

OPENPAGES

i2

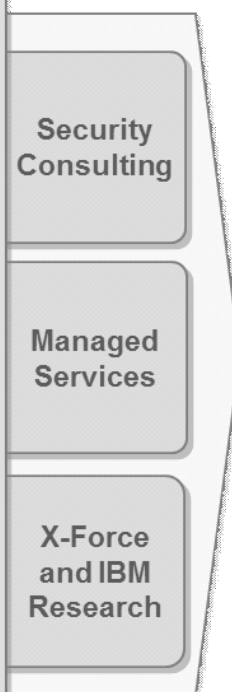
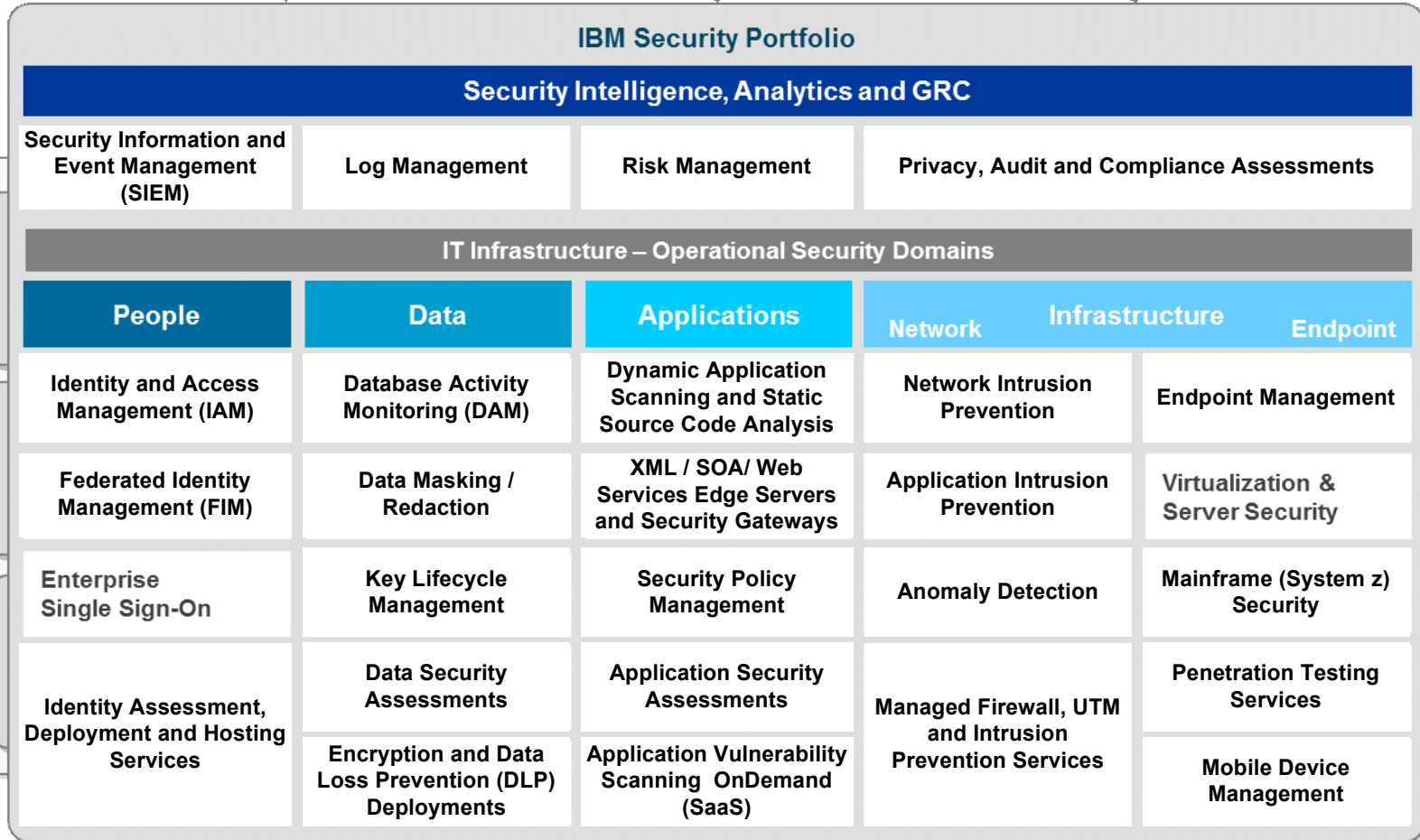
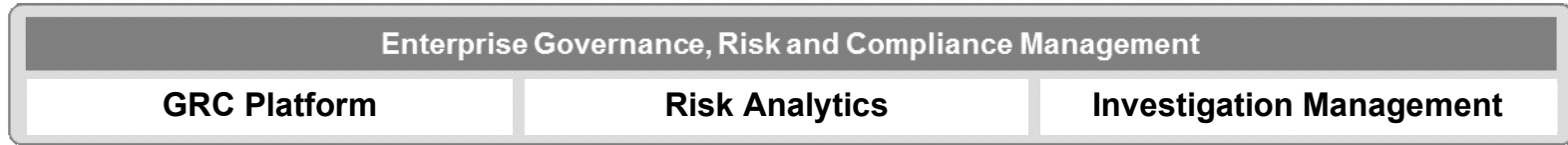
1 Labs

Algorithmics | A



# IBM Security

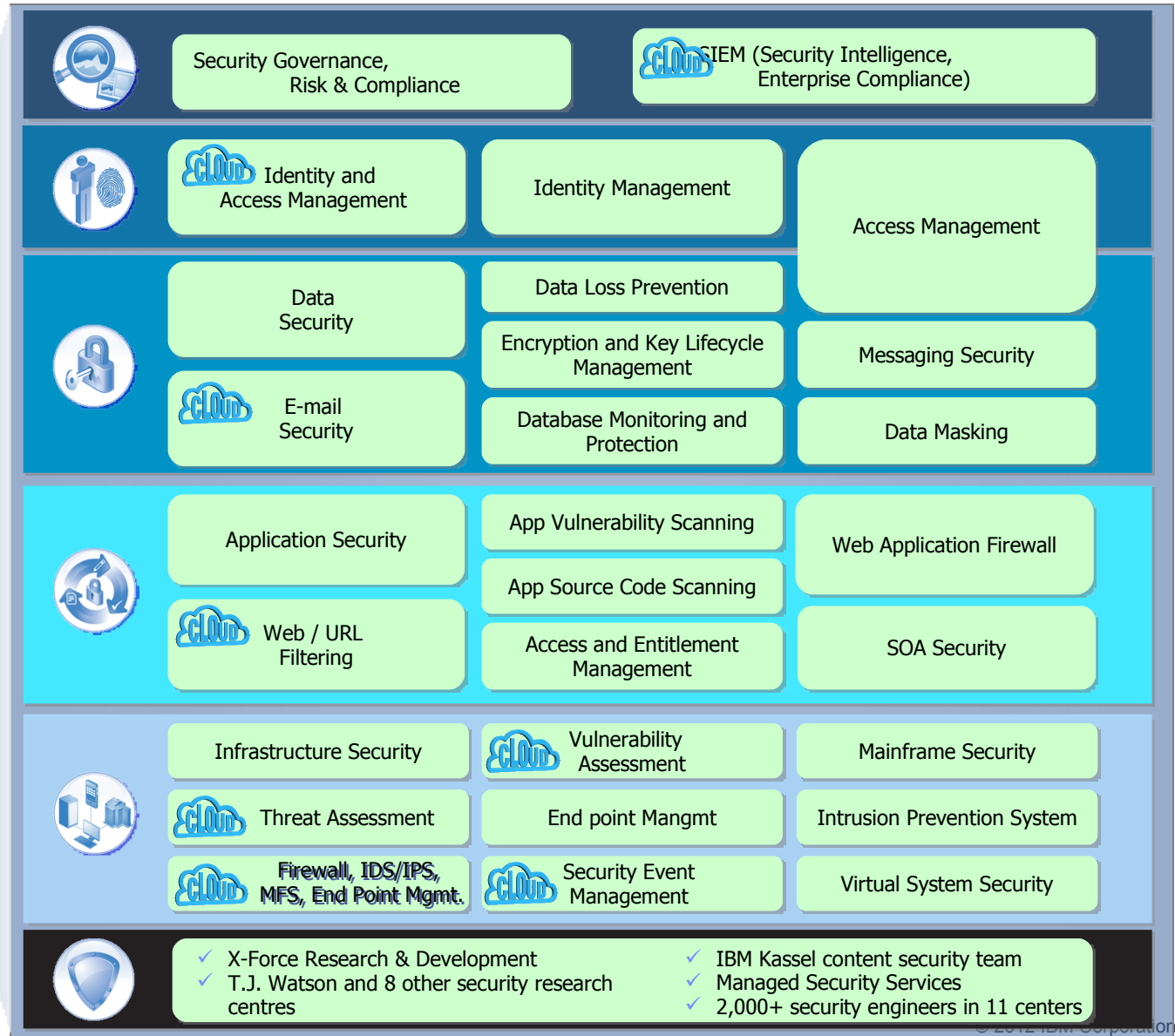
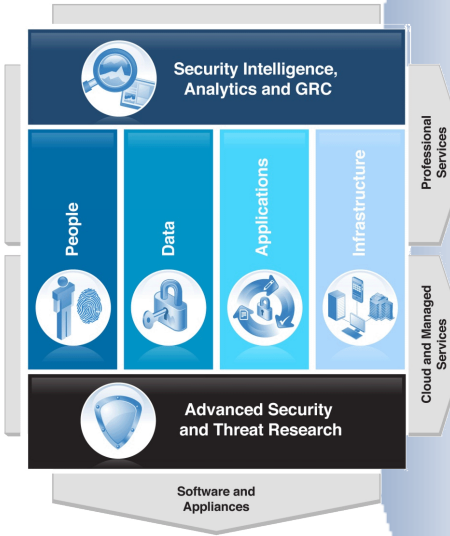
ALERTCON 1



v12-03



**ALERTCON 1**






ALERTCON 1



# IBM's internal approach as an enterprise and service provider

*Focused on security essentials, informed by the IBM Security Framework*

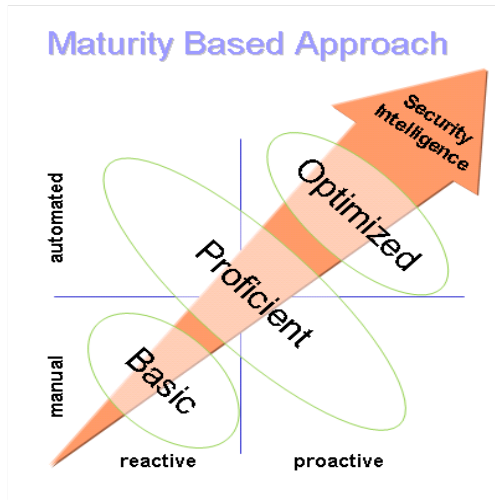


1. Build a risk-aware culture and management system



6. Control network access and help assure resilience



2. Manage security incidents with greater intelligence





7. Address new complexity of cloud and virtualization





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"

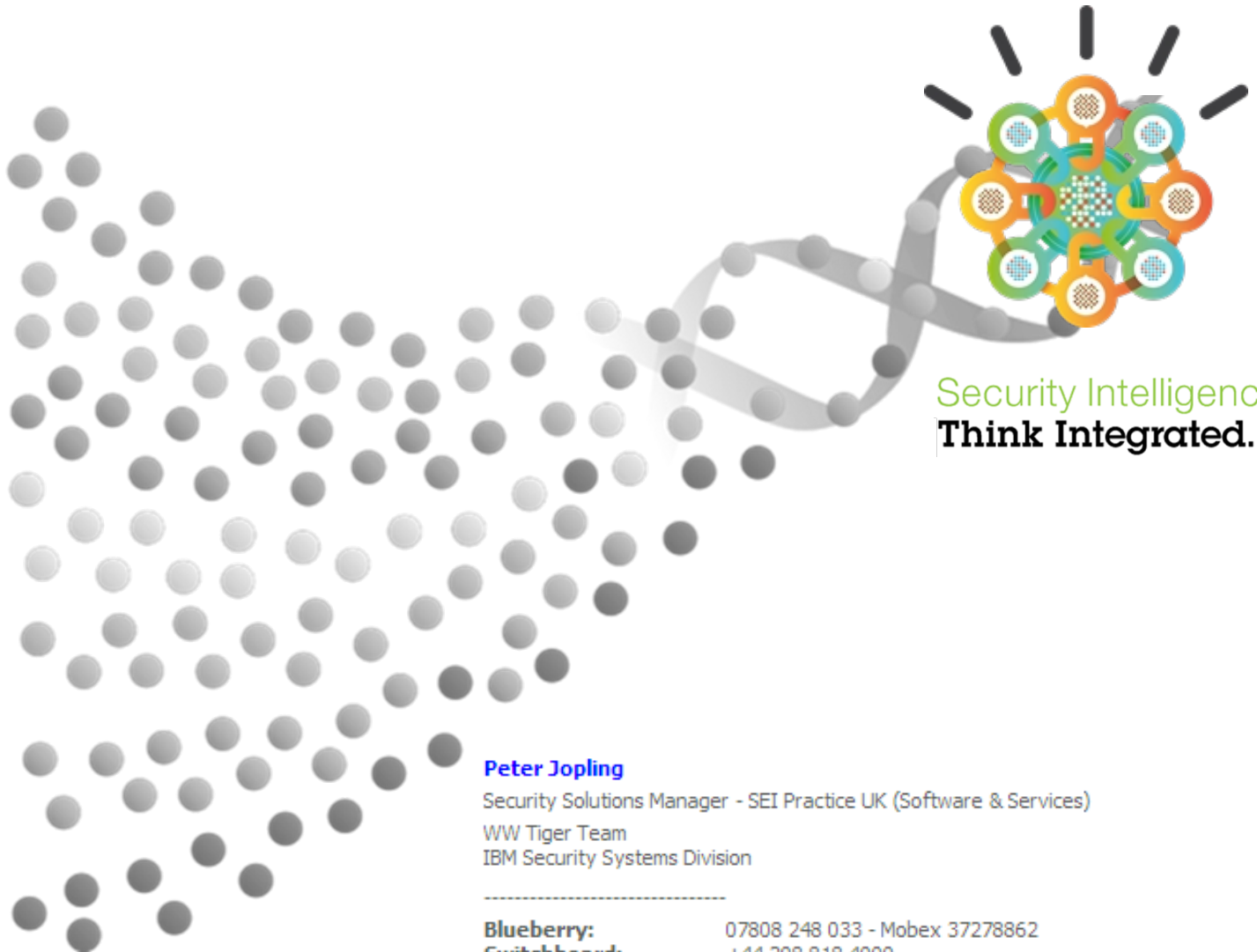
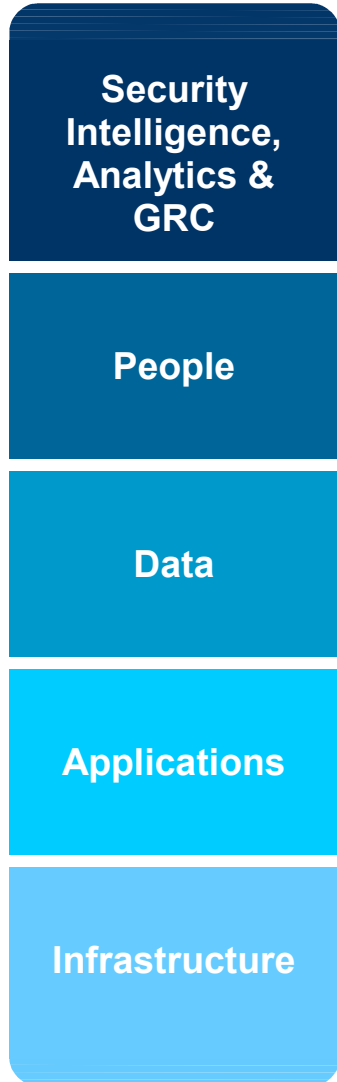
10. Manage the identity lifecycle





# Integrated security thinking from IBM

ALERTCON 1



Security Intelligence.  
**Think Integrated.**

**Peter Jopling**

Security Solutions Manager - SEI Practice UK (Software & Services)  
WW Tiger Team  
IBM Security Systems Division

**Blueberry:**  
**Switchboard:**  
**e-mail:**  
**Snail Mail:**

07808 248 033 - Mobex 37278862  
+44 208 818 4000  
joplingp@uk.ibm.com  
MP135, Galileo Building, IBM Hursley, Winchester, UK