IBM Forum Segrate - Milano

18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

Andrea Carmignani e Giovanni Todaro

Le sfide del CISO

With explosive growth in connectivity and collaboration, information security is becoming increasingly complex and difficult to manage

In 2011, the corporate world experienced one of highest data loss total

The number of mobile workers is expected to reach 1.3 billion by 2015

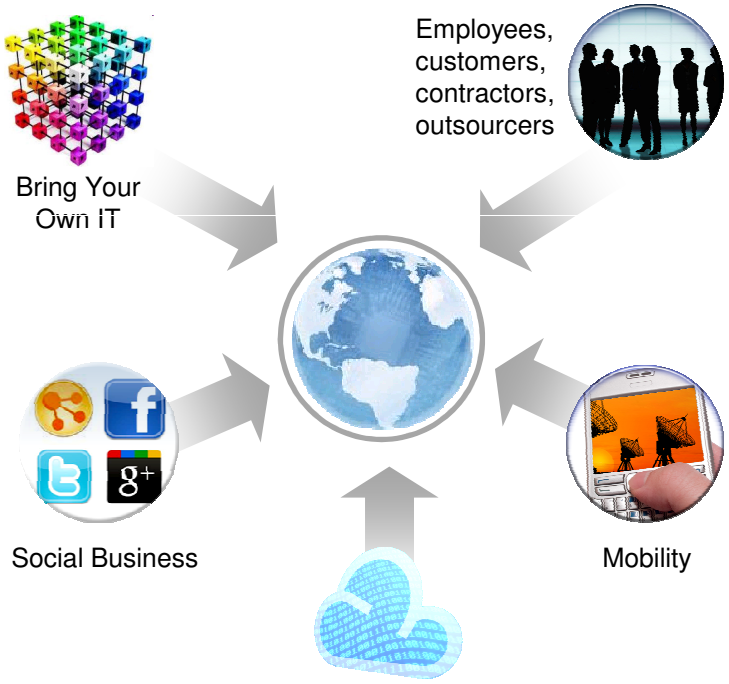
At the same time, mobile security threats are increasing – up almost 20 percent in 2011

Sources: Verizon 2012 Data Breach Investigations Report; IDC

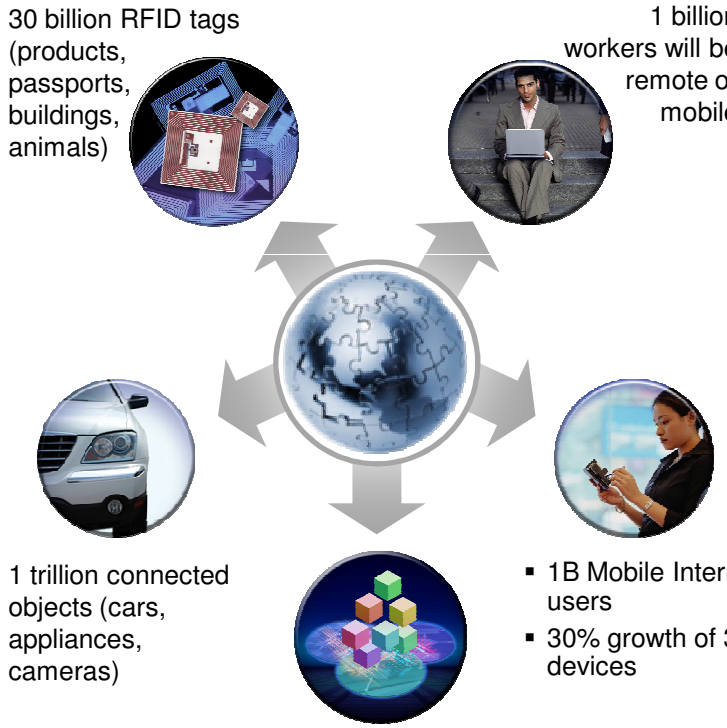
© 2012 IBM Corporation

Number of Vulnerabilities increase radically with emergence of mobile, cloud, BYOD

Embracing New Technologies, Adopting New Business Models



Exploding and Interconnected Digital Universe



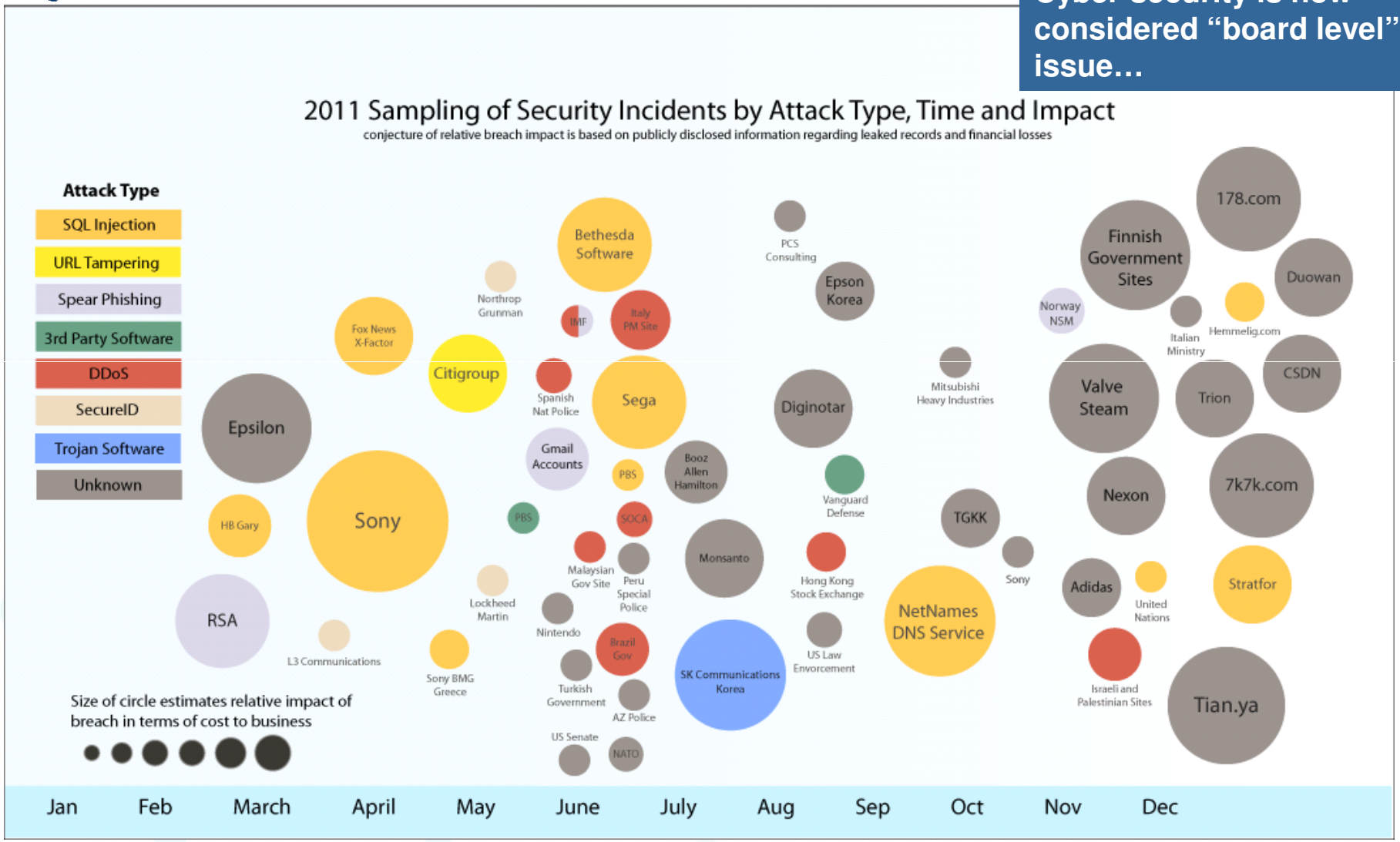
33% of all new business software spending will be Software as a Service

© 2012 IBM Corporation

Cyber impacts have been increasing in size, scope

2011 Sampling of Security Breaches by Attack Type, Time and Impact

Cyber security is now considered "board level" issue…



"The Year of the Security Breach" – IBM's X-Force® R&D

© 2012 IBM Corporation

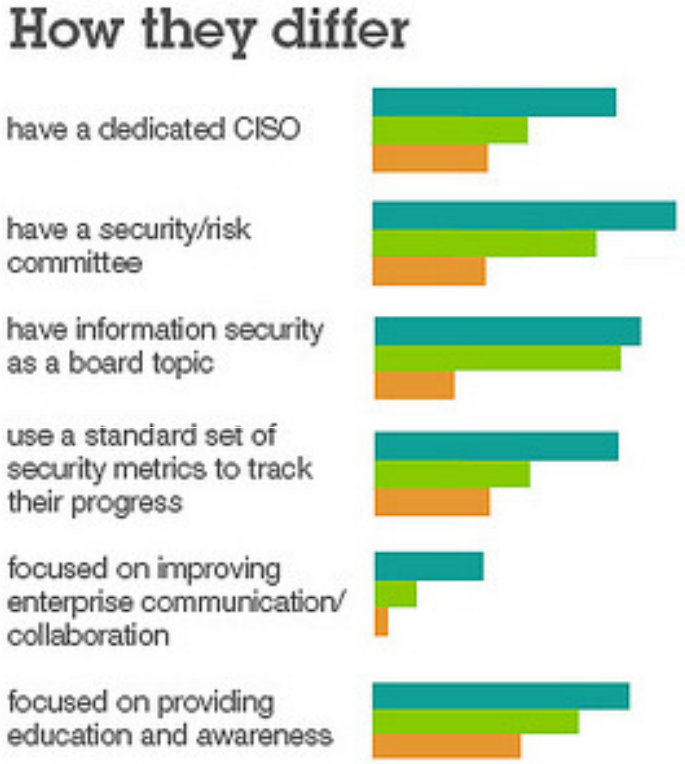
To obtain a global snapshot of security leaders' strategies and approaches, we asked 138 security leaders in…

- *Seven countries*
- *A wide range of industries*
- *~20% from enterprises with 10,000+ employees*
- *~55% from enterprises with 1,000-9,999 employees*

© 2012 IBM Corporation

IBM CISO study revealed critical shift in the role of Chief Information Security Executives globally

- Influencers (25%) => **RISK**
- Protectors (47%) => **COMPLIANCE**
- Responders (28%) => **CRISIS**



Building a business case: *According to Gartner, average security spend = **5-9%** of overall IT budget. The more mature, the less they spend.*

© 2012 IBM Corporation

Unfortunately, security skills to help manage heightened security risks are hard to find

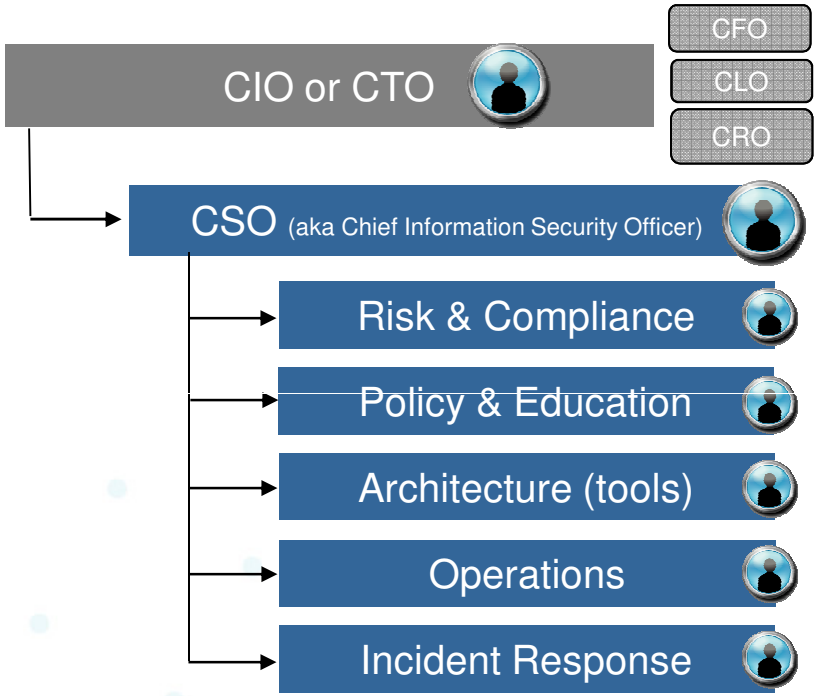
58%

are unable to find people with the right skills

66%

struggle with an understaffed IT team

FORRESTER



81% of CISO functions *are re-organizing or* ***have been re-organized within the last 6 months****. Changes include increased scope, change in reporting line.*

Source: Corporate Executive. Board, IREC Study, July 2012

© 2012 IBM Corporation

Security leaders must assume a business leadership position and dispel the idea that information security is a technology support function

Responders can move beyond their tactical focus by:

- Establishing a dedicated security leadership role (like a CISO), assembling a security and risk committee, and measuring progress
- Automating routine security processes to devote more time and resources to security innovation

Protectors can make security more of a strategic priority by:

- Investing more of their budgets on reducing future risks
- Aligning information security initiatives to broader enterprise priorities
- Learning from and collaborating with a network of security peers

Influencers can continue to innovate and advance their security approaches by:

- Strengthening communication, education and business leadership skills to cultivate a more risk-aware culture
- Using insights from metrics and data analysis to identify high-value improvement areas

© 2012 IBM Corporation

10 Essential Practices – Providing Security Defense in Depth

5. Automate Security Hygiene

6. Control Network Access & Assure Resilience

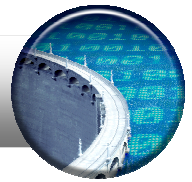
4. Secure Services, By Design

7. Address New Complexity of Cloud and Virtualization

3. Enable the Secure Mobile Workplace

8. Assure Security Compliance

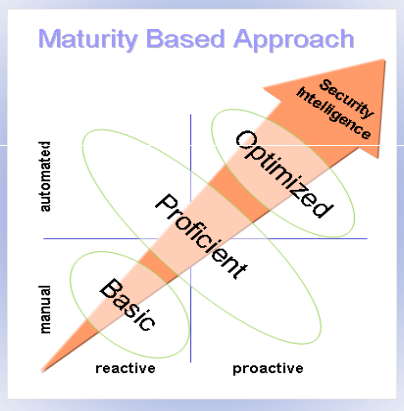
2. Manage Incidents



9. Protect Structured & Unstructured Data

1. Build a Risk Aware Culture & Management System

10. Manage the Identity Lifecycle



© 2012 IBM Corporation

Putting it all together – The Security Framework

Enterprise Governance, Risk and Compliance Management

OpenPages | Algorithmics | i2 Corporation

Security Portfolio

IT Security and Compliance Analytics & Reporting

Security information and event management	Advanced analytics (Streams, SPSS, etc.)	Penetration Testing & Red Team Exercise

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure: Network	Infrastructure: Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Source Code Scanning	Network IDS and host based IPS	Anti-Malware Gateway
Federated Identity Manager	Optim Data Masking	AppScan Application Security Assessment		zSecure Mainframe Security
Enterprise Single Sign-On	Key Lifecycle Management	Worklight Mobile Application Security	Network Firewall	Server Security (Tivoli Endpoint Manager)
Role Based Analytics/SOD checking	Encryption	Web Application Firewall	DDOS Protection	Mobile Endpoint Management (Tivoli Endpoint Manager)
	Data Loss Prevention (network & endpoint)	AppScan OnDemand Software as a Service	Content Filtering	

Security Consulting | Implementation Services | Managed Services

© 2012 IBM Corporation

An Italian Company, Sirti has chosen IBM Security Intelligence

CHI SIAMO

Sirti è la società italiana leader nel settore dell'ingegneria e dell' impiantistica di rete.
Sirti offre soluzioni integrate per l'installazione, la costruzione e la manutenzione nei mercati delle Telecomunicazioni, dei Trasporti, dell'Energia e Infrastrutture, anche operanti nel settore ICT.

DATI PRINCIPALI

90	ANNI DI ESPERIENZA
4.100	DIPENDENTI
3.000	UNITA' OPERATIVE
20	GRUPPI OPERATIVI
18	REGIONI CON PRESENZA SIRTI

Sirti

Release Agosto 2012

© 2012 IBM Corporation

An Italian Company, Sirti has chosen IBM Security Intelligence

Sirti has chosen QRadar SIEM which provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

SIM/SEM

QRadar® SIEM

- Integrated log, cyber threat, risk and compliance management
- Sophisticated event analytics
- Asset profiling and flow analytics

•Detect external threats and attacks in real-time via advanced analytics

•Consolidate silos of network and security information to gain a single view across the enterprise.

•Detect potential insider threats (theft, fraud, malicious activity).

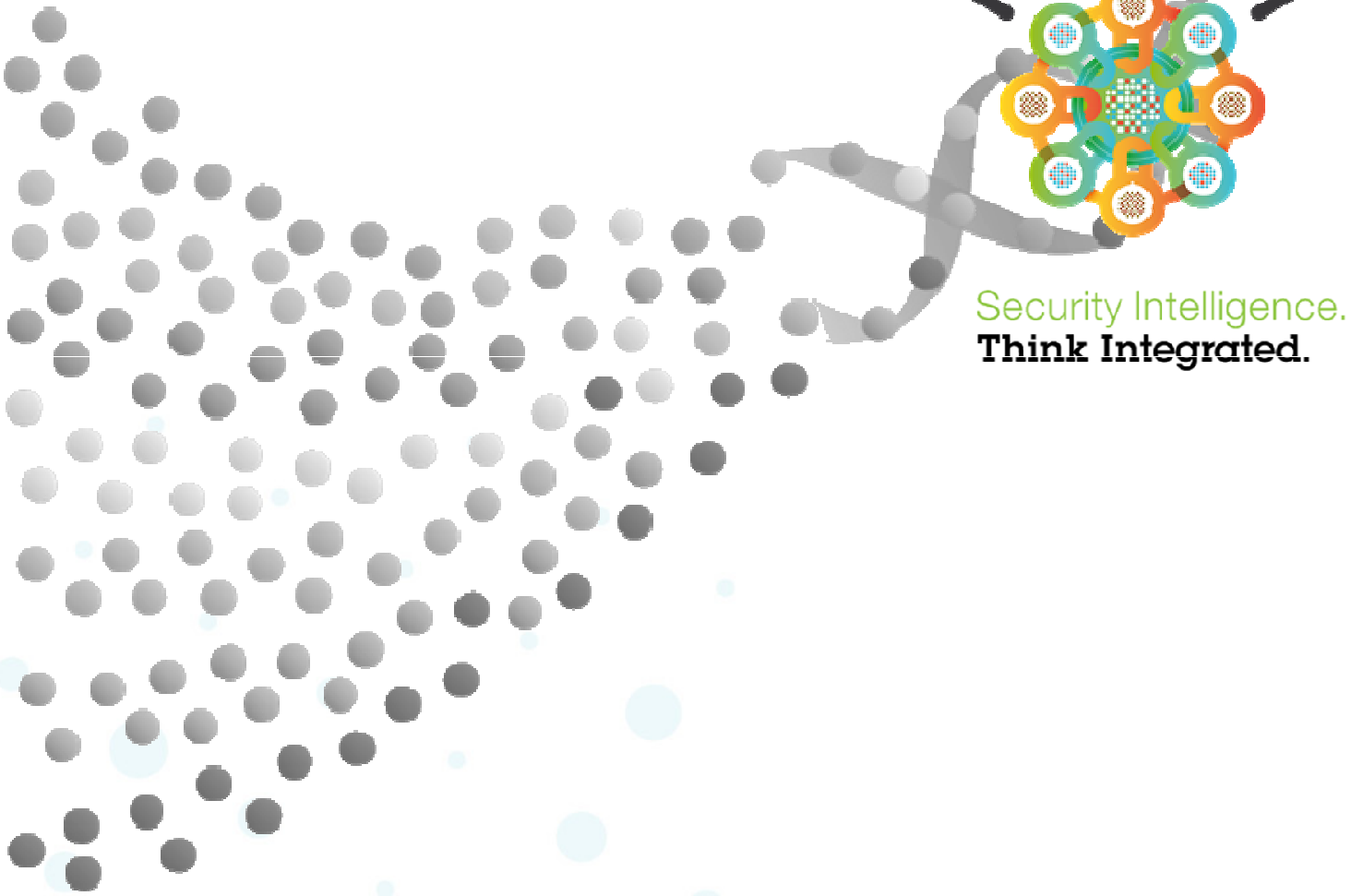
•Lower the costs of managing audits and maintaining compliance with the full set of applicable regulations and policies.

•Minimize the possibility of regulatory non-compliance.

© 2012 IBM Corporation

Intelligent solutions provide the DNA to secure a Smarter Planet

- Security Intelligence, Analytics & GRC
- People
- Data
- Applications
- Infrastructure



Security Intelligence.
Think Integrated.

© 2012 IBM Corporation