IBM Connected 2013

Her Deneyim Bir Kazanım

Stephen Cotrell
IBM Software Group

#connected

Managing threats in the digital age

Addressing security, risk and compliance

November 2013

#connected

Agenda

1 Managing threats in the digital age

2 Addressing security, risk and compliance

3 Taking action

Security has moved from an IT issue to an ongoing business concern

Internal abuse of key sensitive information

WIKILEAKS
Unauthorized release of classified records

IMPACT
Close to $100M for the U.S. Army alone; damaged foreign relations worldwide

Complexity of malware, ability to slowly leak data and affect critical business processes

STUXNET
Targeted changes to process controllers refining uranium

IMPACT
Degraded ability to safely process and control highly volatile materials

External data breach of third party data and theft of customer information

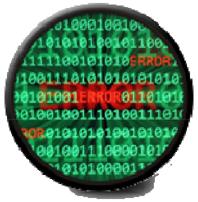
EPSILON
Theft of customer data affected > 100 companies

IMPACT
Up to $4 billion in costs for initial clean-up and longer term litigation risks

What's the risk?

Hackers obtained personal information on 70 million subscribers.

April 2011: *Malicious outsiders stole name, address (city, state, zip), country, email address, birth date, PlayStation Network/Qriocity password and login, and handle/PSN online ID, and possibly credit card numbers from 70 million Sony PlayStation users.*



SQL injection is fast becoming one of the biggest and most high profile web security threats.

April 2011*: A mass SQL injection attack that initially compromised 28,000 websites shows no sign of slowing down. Known as LizaMoon, this malicious code is after anything stored in a database.*

Unprotected test data sent to and used by test/development teams as well as third-party consultants.

February 2009: *An FAA server used for application development & testing was breached, exposing the personally identifiable information of 45,000+ employees.*

Hundreds of thousands of secret reports regarding US wars in Iraq and Afghanistan published on WikiLeaks.

December 2010: *A private in the US military, downloaded top secret military documents and passed them to journalist for publication. This puts US national security at risk as well as the lives of those named in reports.*

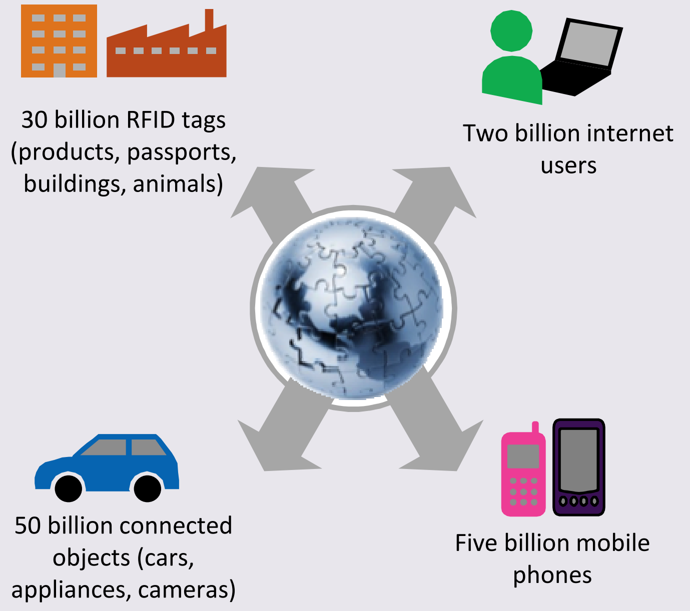
Organizations face difficult decisions

- **Do nothing** … however:
  - Limited time, lots of regulation, growing costs of compliance
  - Requirements for privacy/security by user role add complexity
  - **73%** of security professionals say the volume of database attacks will increase
  - **$7.2M USD** is the average cost of a data breach
  - **95%** of compromised records originated in **database servers**
  - **88%** of organizations surveyed had at least one data breach
- **Leverage home grown approaches** … however:
  - Manual approaches lead to higher risk and inefficiency
  - Requirements for privacy/security by user role add complexity
  - New source of threats: outsourcing, web-facing applications, stolen credentials, insiders
- **Implement a holistic data protect strategy**

> *Don’t focus just on one or two databases but extend your efforts to become enterprisewide — encompassing hundreds and thousands of databases.*
>
> *-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011*

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks

EXPLODING DIGITAL UNIVERSE



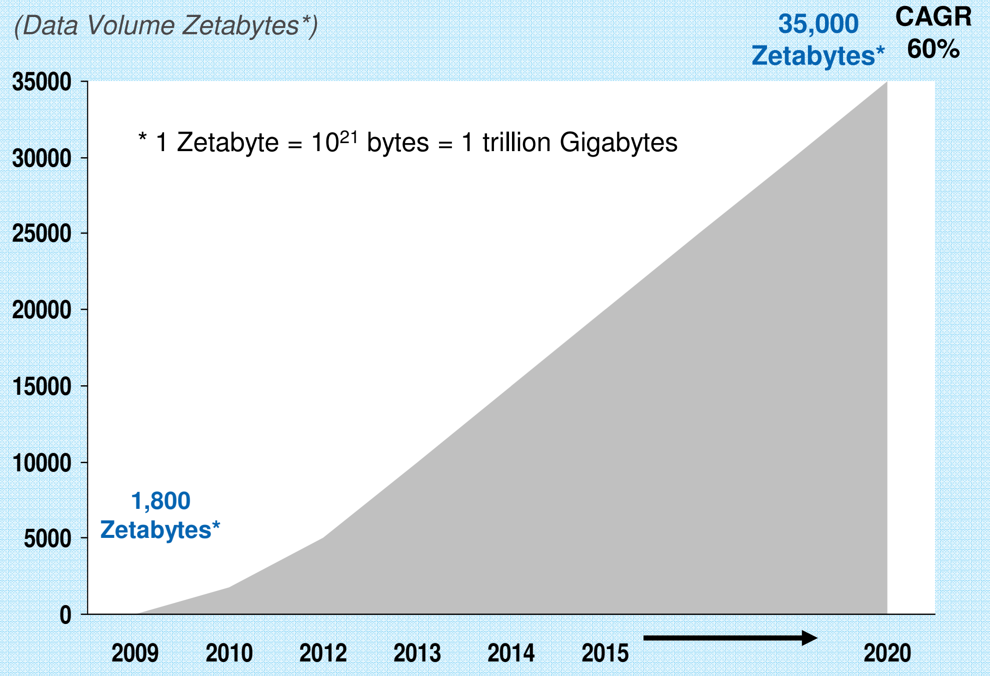
30 billion RFID tags (products, passports, buildings, animals)

Two billion internet users

50 billion connected objects (cars, appliances, cameras)

Five billion mobile phones

WORLDWIDE DATA VOLUMES PROJECTED TO INCREASE 29X OVER 10 YEARS



> *"There are security leaks involving mobile browsers that we don't even know enough about yet."*
>
> \- CIO, Media Company

*Source: International Telecommunications Union. "Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010." United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls; Ericsson. "More than 50 billion connected devices – taking connected devices to mass market and profitability." February 14, 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c; IDC "Digital Universe Study," sponsored by EMC, May 2010

Security challenges are increasing in number and scope…

EXTERNAL THREATS

Sharp rise in external attacks from non-traditional sources

- Cyber attack
- Organized crime
- Corporate espionage
- Government-sponsored attacks
- Social engineering

INTERNAL THREATS

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employees actions
- Mix of private / corporate data

COMPLIANCE

Growing need to address a steadily increasing number of mandates

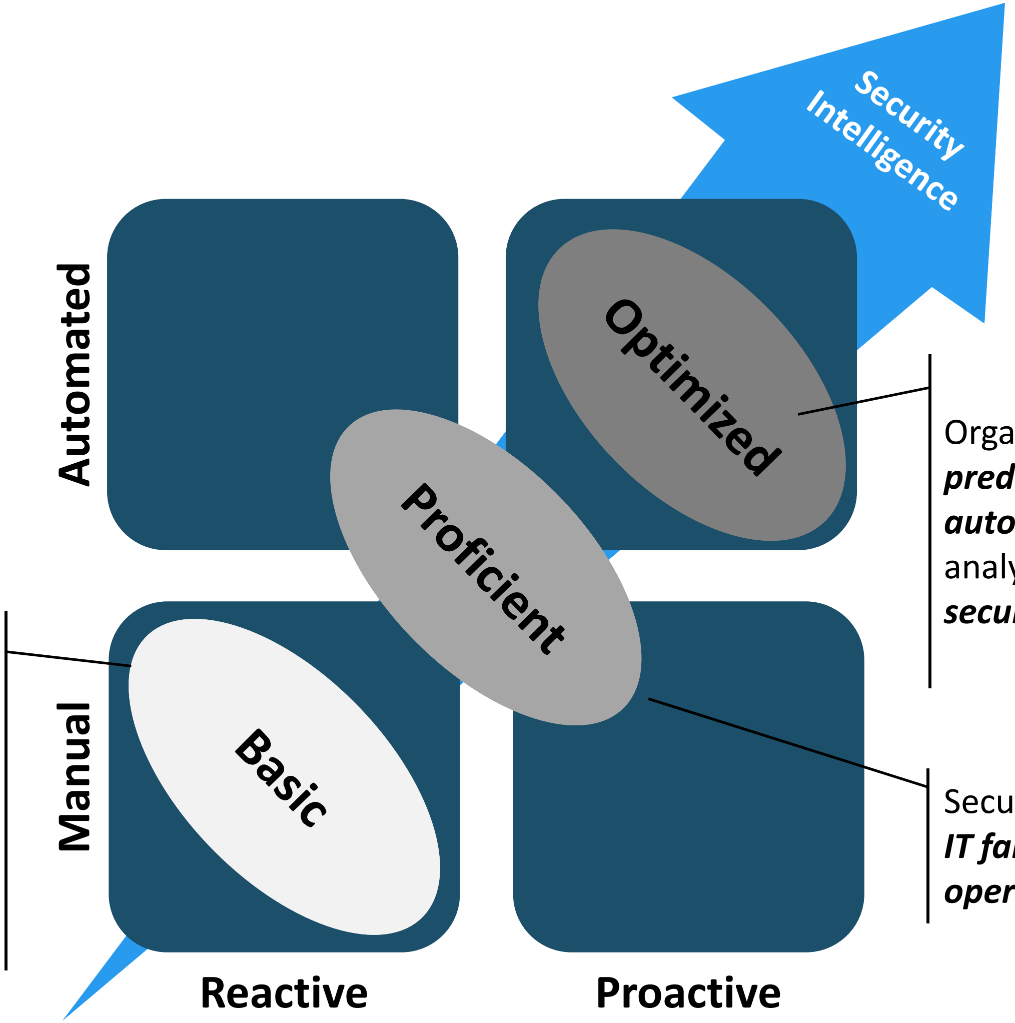
- National regulations
- Industry standards
- Local mandates

…and will continue to have a significant impact on C-level priorities*

	CEO	CFO/COO	CIO	CHRO	CMO
CxO priority	Maintain competitive differentiation	Comply with regulations	Expand use of mobile devices	Enable global labor flexibility	Enhance the brand
Security risks	Misappropriation of intellectual property Misappropriation of business sensitive data	Failure to address regulatory requirements	Data proliferation Unsecured endpoints and inappropriate access	Release of sensitive data Careless insider behavior	Stolen personal information from customers or employees
Potential impact	Loss of market share and reputation Criminal charges	Audit failure Fines, restitutions and criminal charges	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

*Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Increased threats and compliance requirements require more automated, proactive approaches to security…Guardium



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

Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

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

. . .and must take a balanced approach to managing physical, technological and human assets

Security Domains	Today		Tomorrow: Security Intelligence	
People	Manage identities per application	Security Gap	Employ role-based dashboard and privileged user management	Apply advanced correlation and deep analytics
Data	Deploy access control and encryption		Monitor usage and control leakage	
Applications	Scan for vulnerabilities		Build securely from day one	
Infrastructure	Block unwanted network access and viruses		Execute real-time advanced threat detection and forensics	

Reactive ●-----------------▸ **Proactive**

Addressing security issues in the boardroom

GETTING TO SECURITY INTELLIGENCE: A Three Point Plan

1 GET INFORMED

Take a structured approach to assessing business and IT risks

2 GET ALIGNED

Implement and enforce security excellence across the extended enterprise

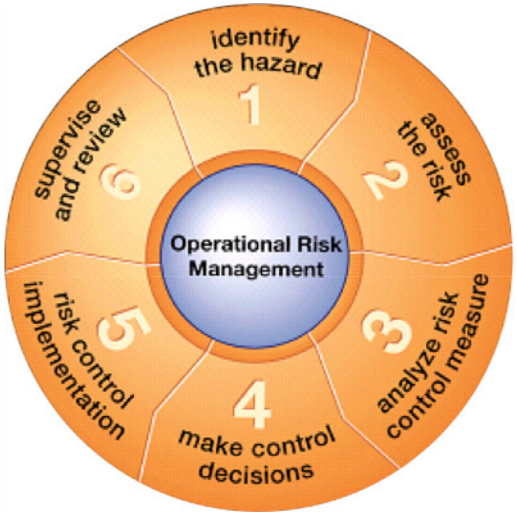
3 GET SMART

Use analytics to proactively highlight risks and identify, monitor and address threats

Take a structured approach to assessing business and IT risks

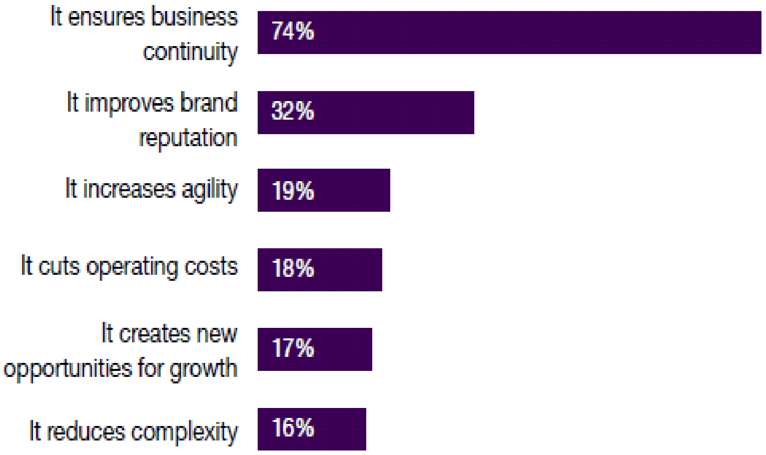
RISK MANAGEMENT FRAMEWORK

2010 IBM Global IT Risk Study


identify the hazard
1
assess the risk
2
analyze risk control measure
3
4
make control decisions
5
risk control implementation
6
supervise and review
Operational Risk Management

THE BENEFITS OF IMPROVING IT RISK MANAGEMENT

2010 IBM Global IT Risk Study



ADDRESSING RISK MANAGEMENT

- Align and integrate IT risk into the business' Enterprise Risk Management framework
- Identify key threats and compliance mandates
- Implement and enforce a risk management process and common controls framework
- Execute incident management processes when crises occurs

EMPOWERING THE RISK EXECUTIVE

- Appoint a C-level executive to manage security risk
- Maintain regular interlock with Board of Directors and peers
- Drive the IT risk conversation into the Enterprise Risk Management program

Client example: A large global financial institution revamped its IT governance and business controls to address audit challenges

SITUATION

A large financial institution:

- Received three adverse opinions from its external auditor, citing significant material issues including significant Sarbanes-Oxley (SOX) weaknesses
- Received multiple adverse IT security reports from its internal auditor
- Needed to implement strong controls based on industry best practices to address adverse audit reports and ensure the controls were regularly updated and improved

ACTION

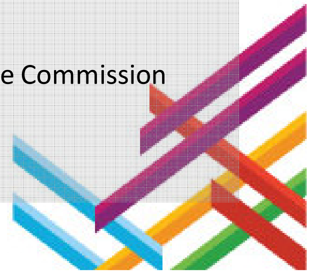
Working with the CEO and CIO, IBM:

- Assessed information security governance by reviewing security processes and writing/updating policies, standards, and procedures
- Closed gaps identified by the assessment by establishing four IT governance committees, writing the committee charters, policies and procedures, and chairing the initial meetings until the client was comfortable taking them over
- Applied IBM's deep subject matter expertise and experience in implementing COBIT® to oversee quality control for contractors implementing business and IT controls

RESULT

The financial institution implemented an IT governance program with strong IT and business controls based on COBIT®

- Achieved a clean financial statement audit and SOX opinion from its external auditor
- This allowed the company to register a new common stock offering with the Securities and Exchange Commission (SEC) which increased investor confidence and increased its stock value.
- Institutionalized the IT governance lifecycle program to ensure continuous improvement



Implement and enforce security excellence across the extended enterprise

EXTENDED ENTERPRISE

CUSTOMERS

- Develop and communicate personal information policies
- Rapidly address privacy breaches

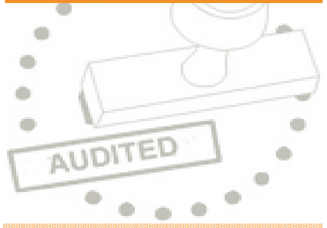
EMPLOYEES

- Set clear security and privacy expectations
- Provide education to identify and address risks
- Manage and monitor system and data access

PARTNERS

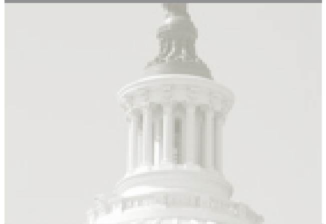
- Set security and privacy expectations
- Provide rapid incident transparency and response
- Report on, and manage risk as part of normal business activities

AUDITORS



- Ensure IT risk aligns with enterprise risk
- Contribute to control framework
- Conduct regular regulatory and company policy reviews

REGULATORS



- Manage regulatory risk
- Demonstrate compliance with existing regulations
- Review and modify existing controls based on changing requirements

Client example: A U.S. health insurer becomes compliant with industry directives and governmental regulations

SITUATION

Faced with a multitude of audits each year, the company needed to respond to audits more consistently and reduce the impact on the business

- Establish compliance with new insurance industry regulatory requirements
- Implement an appropriate IT governance program to address these issues, given the central role IT played in the running of the business

ACTION

IBM worked with the Vice President and Information Compliance Officer and Business Unit Leaders to:

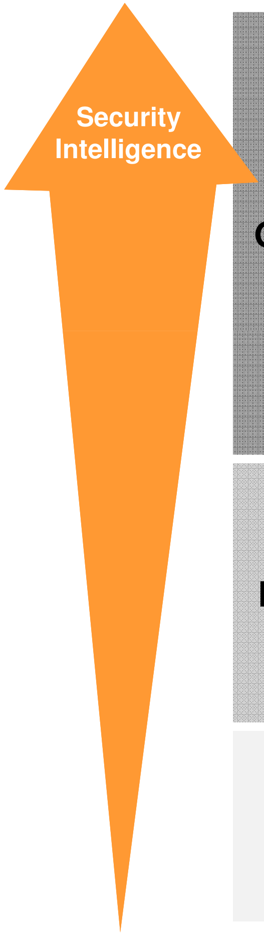
- Institute industry-standard IT governance controls that span all of the company’s operations and business units
- Establish the standards for business partner Service Level Agreements
- Align business and IT, manage risk and ensure security in addition to compliance based on IT audit recommendations
- Monitor compliance with industry regulations and standards (e.g., HIPAA, NAIC Model Audit Rule)
- Implement IBM Security Access Manager for ebusiness

RESULT

As a result, the organization:

- Reduced the effort needed for audit response by approximately 50%;
- Created a more effective, uniform response to audits that: supports regulatory compliance; imparts knowledge transfer through a collaborative “coaching” relationship; and implements IT governance company-wide

Use analytics to proactively highlight risks and identify, monitor and address threats



	People	Data	Applications	Infrastructure
Optimized	Governance, risk and compliance		Advanced correlation and deep analytics	
	Role-based analytics Privileged user controls	Data flow analytics Data governance	Secure application development Fraud detection	Advanced network monitoring/forensics Secure systems
Proficient	Identity management Strong authentication	Activity monitoring Data loss prevention	Application firewall Source code scanning	Asset management Endpoint / network security management
Basic	Passwords and user identities	Encryption Access control	Vulnerability scanning	Perimeter security Anti-virus

Client example: A global pharmaceutical company uses analytics to upgrade its security risk capabilities

SITUATION

A client needed a smarter way to address threats while reducing the cost and complexity of a multi-vendor security environment

- A lack of correlation between reported threats and vulnerability data made it difficult to identify truly critical incidents
- Skilled resources were needed to proactively monitor alerts real-time from multiple security devices and take action before a breach occurs

ACTION

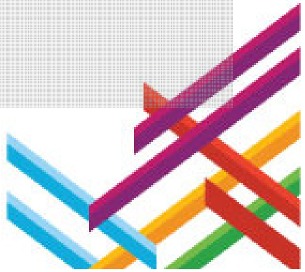
Using IBM's Managed Services, IBM Intrusion Prevention and IBM X-Force Research:

- Millions of multi-vendor security events were analyzed across the customer's computing environment
- Sophisticated analytics processed real-time security event data
- Expert remediation guidance was used to rapidly correct issues and reduce vulnerability windows
- Reports allowed the organization to track and trend vulnerability and threat data over time to gain a broader view of their security posture

RESULT

In addition to taking a more proactive approach to threat management, the client has reduced its security management costs by 57%

- Reduced critical security events from 10,000 events per day to 15
- Consolidated five vendor environments to one



Security is a C-suite responsibility

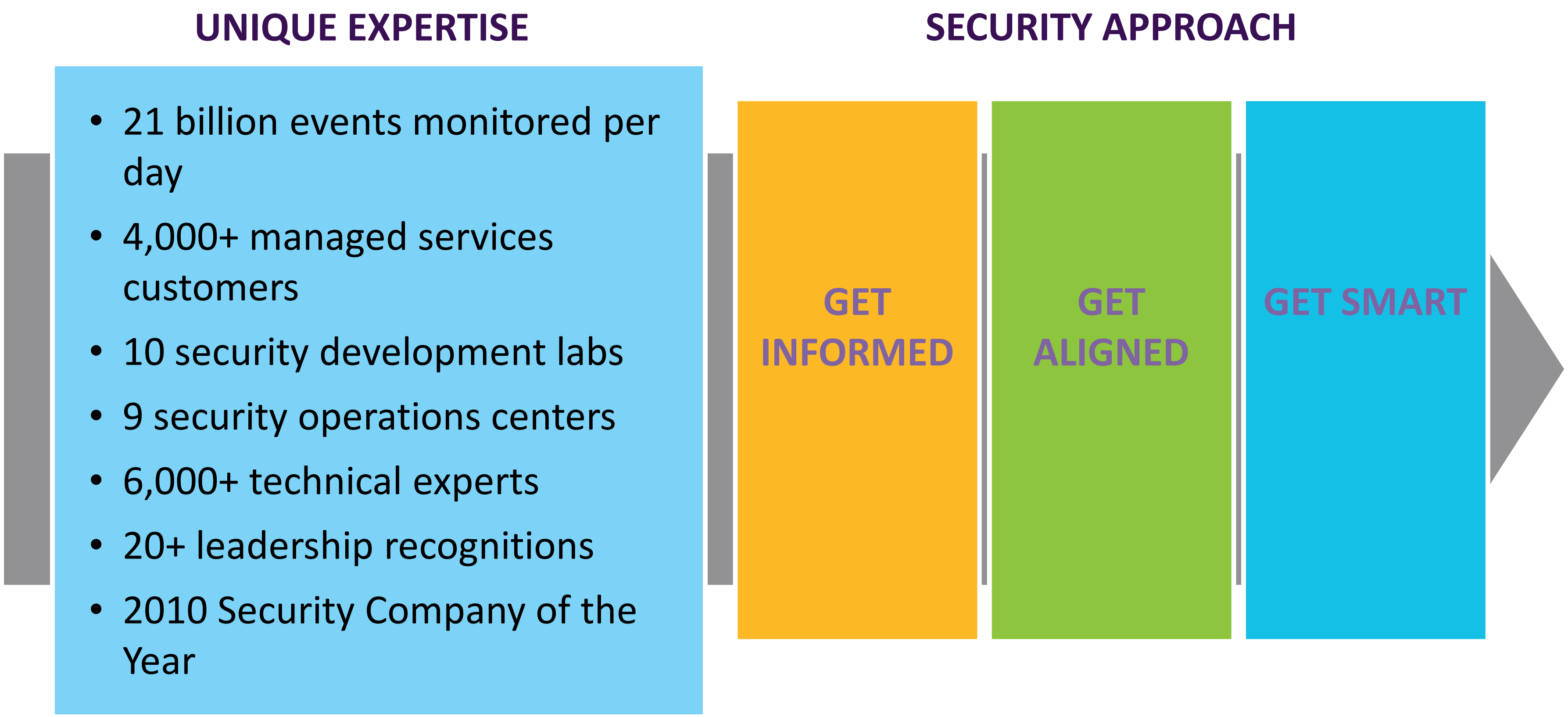
CEO	CFO	COO	CIO	CHRO	CMO
Prevent security risks from impacting shareholder value and trust	Know the financial implications of adverse security events	Evaluate impact of IT systems disruptions on ongoing operations	Understand the fallout effects of information security lapses across the business	Determine risks associated with unwarranted release of employee data	Address brand issues associated with security breaches

Prioritize the security risk management by business impact, instead of trying to protect against every conceivable threat

Where do you stand today?

People	1. To what extent have you rolled out an identity program? 2. How do you know what authorized users are doing? 3. What is your plan to automate identity and role-based management?	1. What is your plan to assess your security risks? 2. How do you detect threats and report compliance across domains? 3. Do you have a log retention and audit capability? 4. Which processes do you use to handle incident response and disaster recovery? 5. How do you involve key internal and external stakeholders in security matters?
Data	1. In what ways have you classified and encrypted sensitive data? 2. How do you know if sensitive data leaves your network? 3. How do you monitor (privileged) access to data?	
Applications	1. How is security built into your application development process from day one? 2. How do you regularly test your website for vulnerabilities? 3. What is your approach to test legacy applications for potential exposures?	
Infrastructure	1. How do you promptly patch connected devices? 2. In what ways do you monitor in- and out-bound network traffic? 3. How are you building security into new initiatives (such as cloud, mobile and the like)?	

IBM's unique security expertise and approach…



UNIQUE EXPERTISE

- 21 billion events monitored per day
- 4,000+ managed services customers
- 10 security development labs
- 9 security operations centers
- 6,000+ technical experts
- 20+ leadership recognitions
- 2010 Security Company of the Year

SECURITY APPROACH

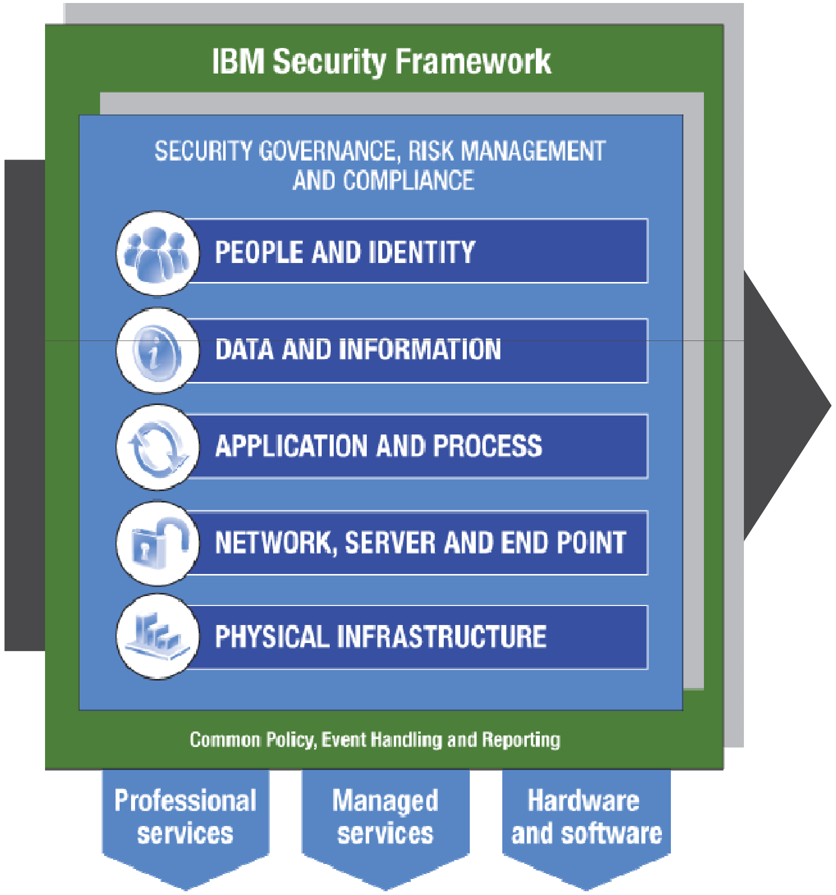
GET INFORMED

GET ALIGNED

GET SMART

…is combined with IBM's depth of capabilities

THE IBM SECURITY FRAMEWORK



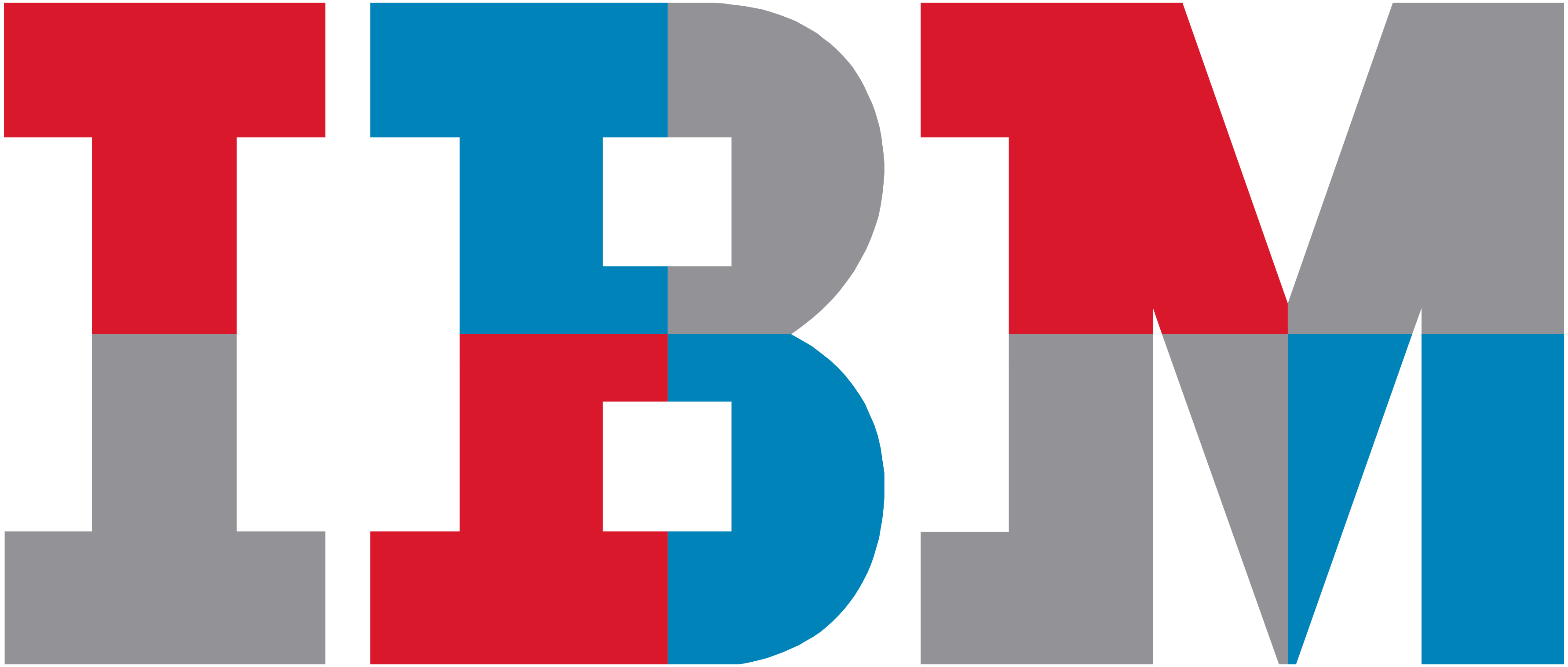
DEPTH OF CAPABILITY

SECURITY CONTROLS

- Governance
- Risk assessments
- Business and IT processes
- Security architecture
- Privacy assessments
- Patch management
- Application security
- Data security/integrity
- Data leakage/loss prevention
- Endpoint security
- Network security
- Identity and access management
- Incident management
- Resiliency management
- Digital video surveillance

SECURITY INTELLIGENCE

- Advanced persistent threat analysis
- Continuous monitoring
- Vulnerability assessments
- Third-party ethical hacking
- Advanced security analytics
- Managed security services
- Security event management
- X-Force Intelligence


IBM