

Security Intelligence.  
**Think Integrated.**

# IBM Security Services

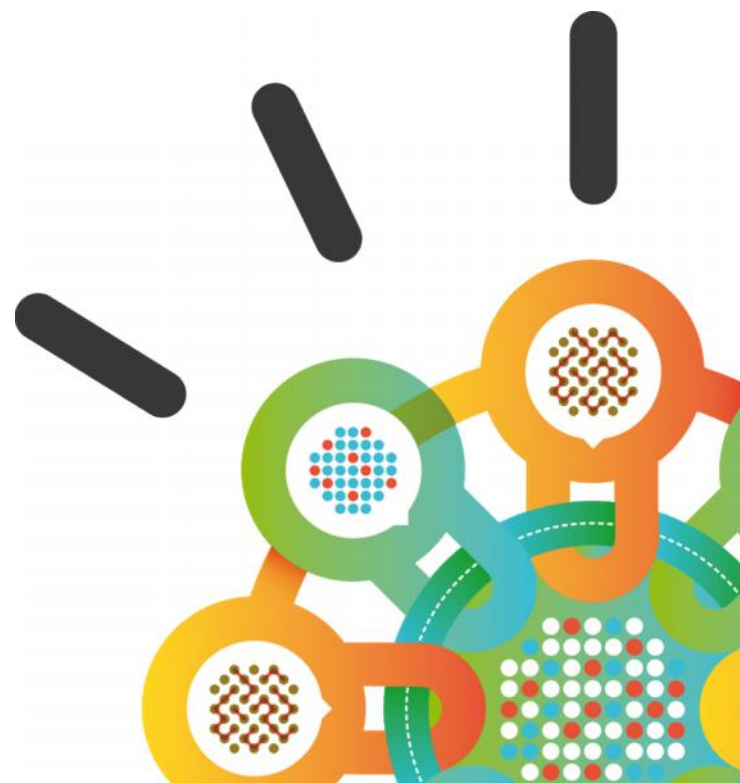
## 10 Essential Security Practices

Stewart Cawthray

Chief Security Architect – IBM Security Services (Canada)

[cawthray@ca.ibm.com](mailto:cawthray@ca.ibm.com)

 [@stewartcawthray](https://twitter.com/stewartcawthray)





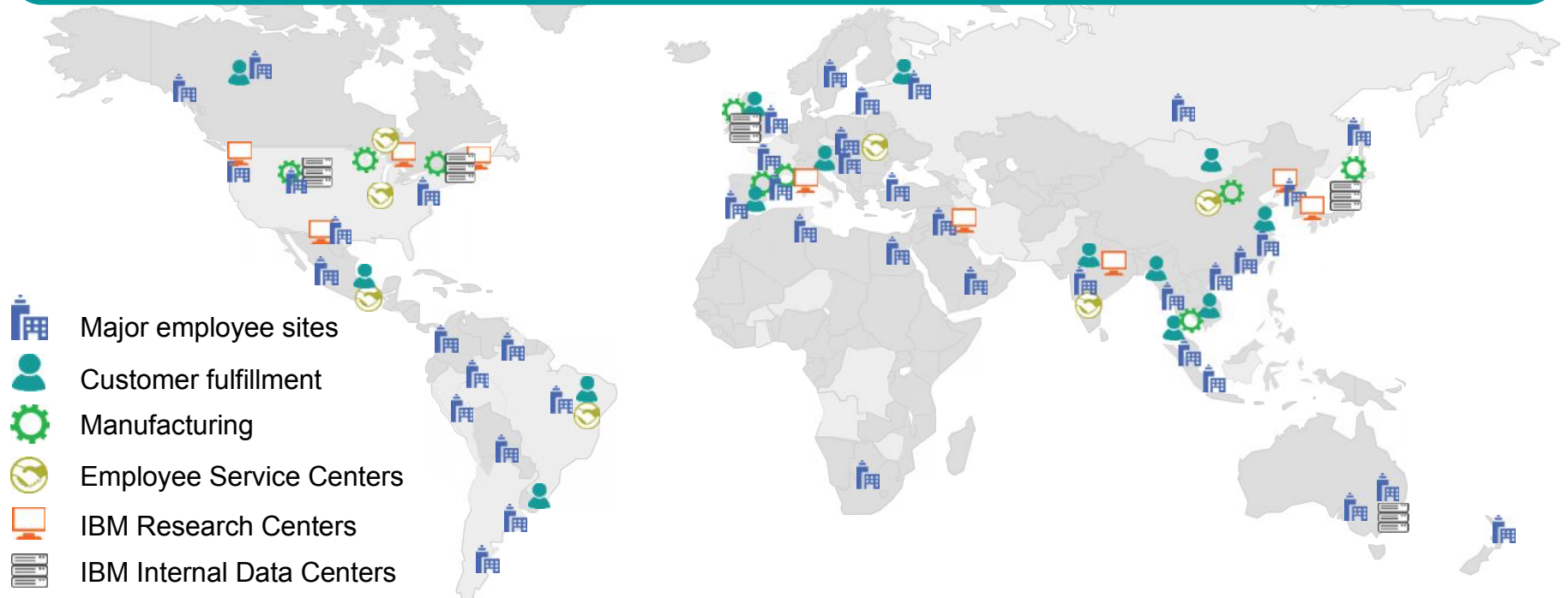
# The enterprise today



# IBM is well qualified to secure the enterprise.

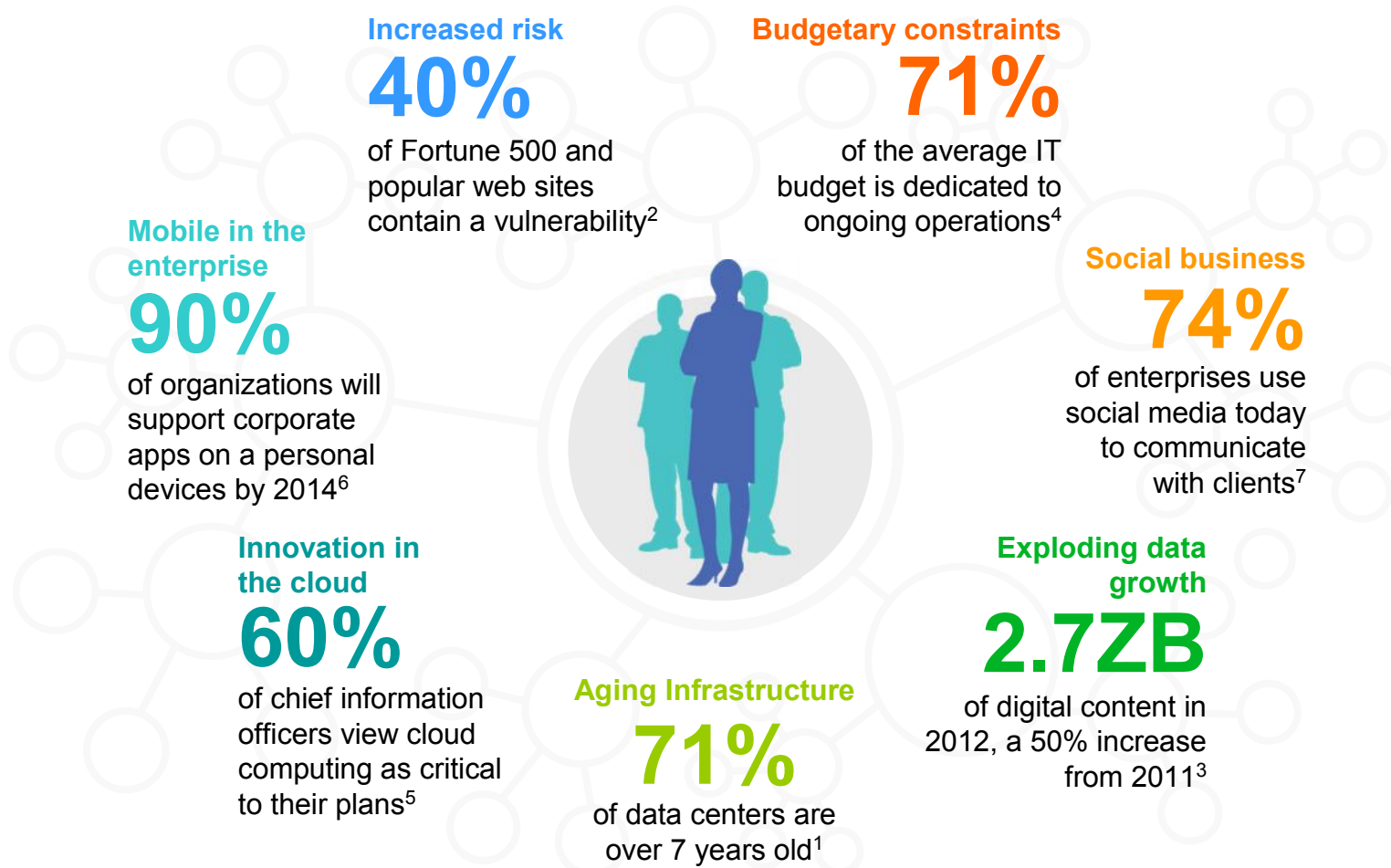
## One of the largest and most complex internal IT infrastructures in the world

- 2,000-plus major sites
- 400,000-plus employees
- 800,000-plus traditional endpoints
- 170-plus countries
- About 200,000-plus contractors
- About 50 percent of employees are mobile





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



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

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**.

# 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

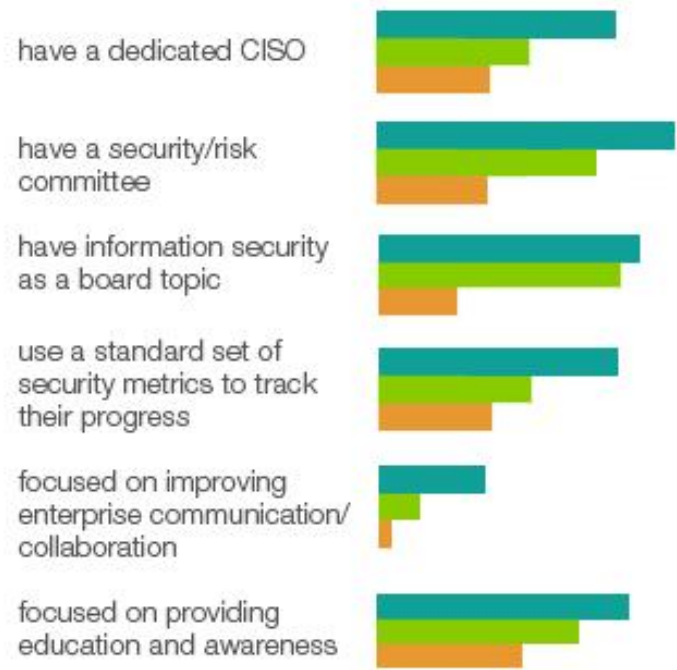
## Protectors

Less confident, prioritize security strategically but lack necessary structural elements

## Responders

Least confident, focus largely on protection and compliance


## How they differ





# The changing dynamics of securing the enterprise

## Today's threats (actors) are more sophisticated.

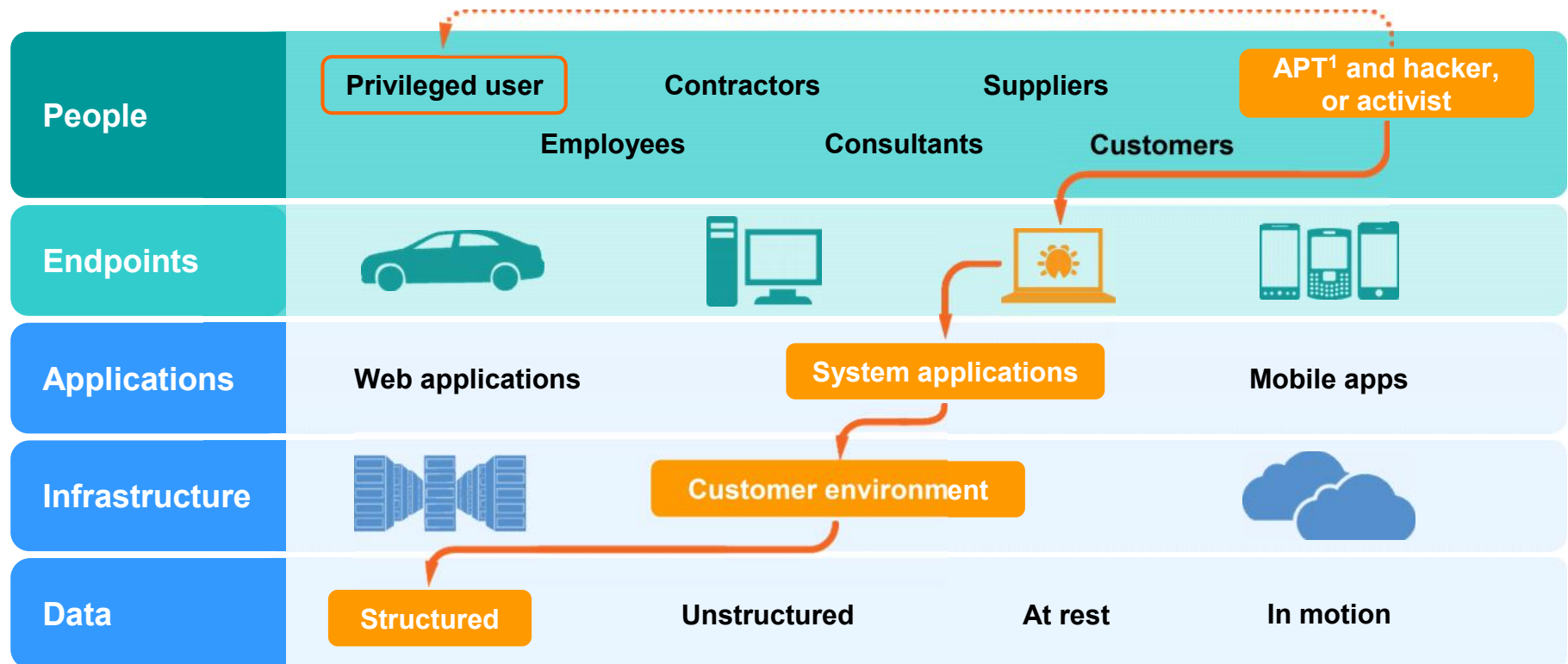
	Threat	Type	% of Incidents	Threat Profile
 Potential Impact	Advanced, Persistent Threat / Mercenary	<ul style="list-style-type: none"> <li>National governments</li> <li>Organized crime</li> <li>Industrial spies</li> <li>Terrorist cells</li> </ul>	Equals less than 10 percent	<ul style="list-style-type: none"> <li>Sophisticated tradecraft</li> <li>Foreign intelligence agencies, organized crime groups</li> <li>Well financed and often acting for profit</li> <li>Target technology as well as information</li> <li>Target and exploit valuable data</li> <li>Establish covert presence on sensitive networks</li> <li>Difficult to detect</li> <li><b>Increasing in prevalence</b></li> </ul>
	Hacktivist	<ul style="list-style-type: none"> <li>"White hat" and "black hat" hackers</li> <li>"Protectors of "Internet freedoms"</li> </ul>	Equals less than 10 percent	<ul style="list-style-type: none"> <li>Inexperienced-to-higher-order skills</li> <li>Target known vulnerabilities</li> <li>Prefer denial of service attacks BUT use malware as means to introduce more sophisticated tools</li> <li>Detectable, but hard to attribute</li> <li><b>Increasing in prevalence</b></li> </ul>
	Opportunist	<ul style="list-style-type: none"> <li>Worm and virus writers</li> <li>Script Kiddie</li> </ul>	20 percent	<ul style="list-style-type: none"> <li>Inexperienced or opportunistic behavior</li> <li>Acting for thrills, bragging rights</li> <li>Limited funding</li> <li>Target known vulnerabilities</li> <li>Use viruses, worms, rudimentary Trojans, bots</li> <li>Easily detected</li> </ul>
	Inadvertent Actor	<ul style="list-style-type: none"> <li>Insiders - employees, contractors, outsourcers</li> </ul>	60 percent	<ul style="list-style-type: none"> <li>No funding</li> <li>Causes harm inadvertently by unwittingly carrying viruses, or posting, sending or losing sensitive data</li> <li>Increasing in prevalence with new forms of mobile access and social business</li> </ul>

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



## Here is the anatomy of a targeted attack.

- Adversary compromises endpoint used by a systems administrator with undetectable malware.
  - The malware has two components:
    - 1) A keystroke logger to capture credentials
    - 2) Command and control capability
- With credentials and command and control malware, adversary impersonates the Sys Admin to gain privileged access to systems and data.
- Data is stolen, and production systems are further compromised.



<sup>1</sup>Advanced persistent threat (APT)

## Here are the top reasons why compromises occur.

### End users and endpoints

- Double-clicking “on anything”
- Disabling endpoint security settings
- Using vulnerable, legacy software and hardware
- Failing to install security patches
- Failing to install anti-virus
- Failing to report lost or stolen device
- Connecting endpoint to a network from an insecure access point (such as Starbucks)
- Using a second access point (such as AirCard), creating a bypass
- Using weak or default passwords, or using business passwords for personal use
- Revealing passwords over the phone

### Infrastructure

- Connecting systems and virtual images to the Internet before hardening them
- Connecting test systems to the Internet with default accounts or passwords
- Failing to update or patch systems/applications on a timely basis.
- Failing to implement or update virus detection software
- Using legacy or end-of-life software and hardware
- Running unnecessary services
- Using insecure back-end management software
- Failing to remove old/unused user accounts
- Implementing firewalls with rules that don't stop malicious or dangerous incoming or outgoing traffic
- Failing to segment network and/or adequately monitor/block malicious traffic with IDS/IPS<sup>1</sup>

**Up to 80-90 percent of all security incidents can be easily avoided!<sup>2</sup>**

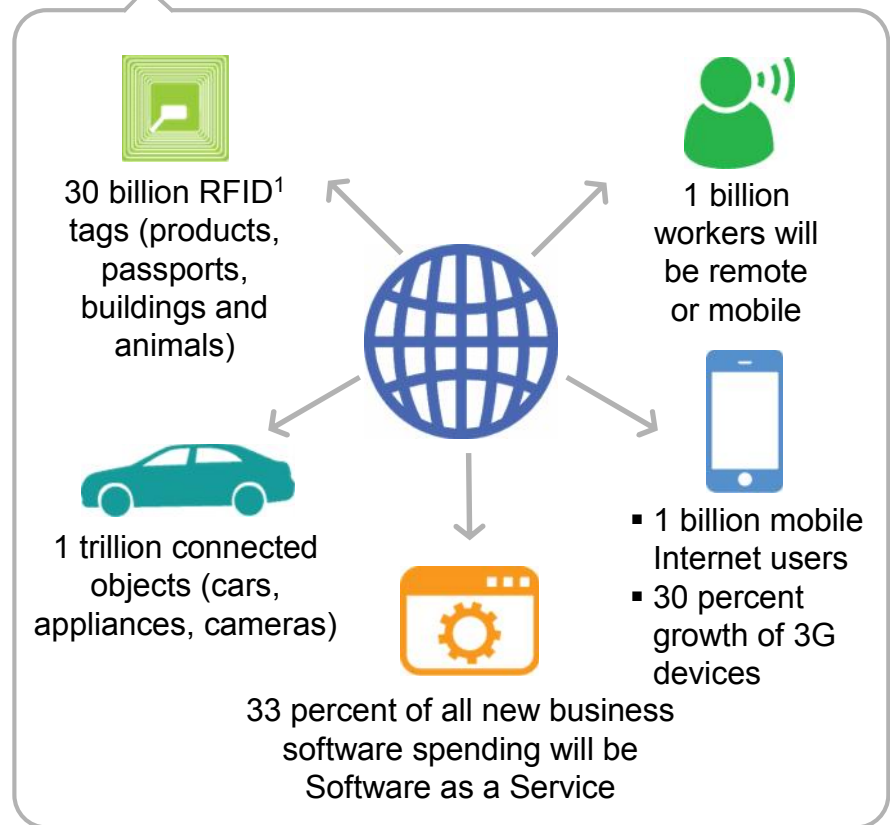
<sup>1</sup>Intrusion detection system and intrusion protection system' <sup>2</sup>Based on IBM X-Force® Trend Report, 2011

# Number of vulnerabilities increase radically with emergence of new business models and technologies.

## Adopting new business models and embracing new technologies



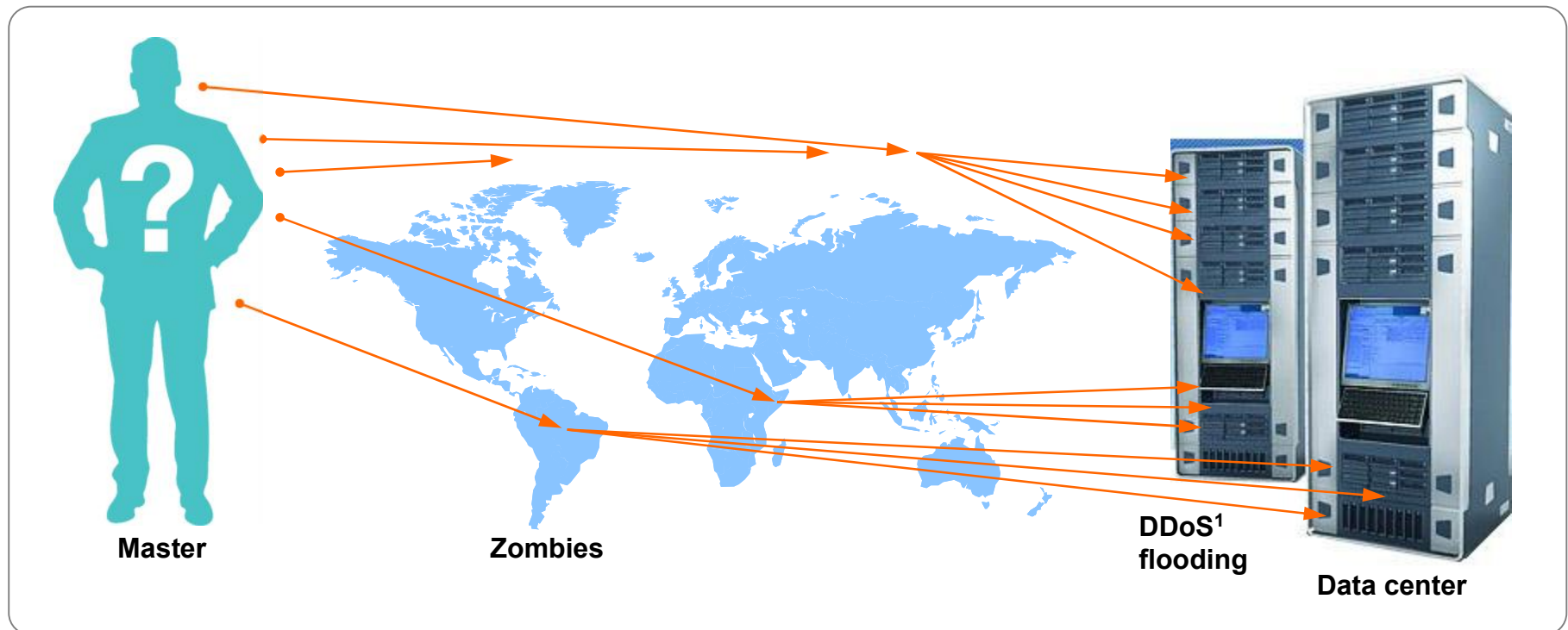
## Exponentially growing and interconnected digital universe



Source: IBM X-Force® Trend Report, 2011

## Here is the anatomy of a denial-of-service attack.

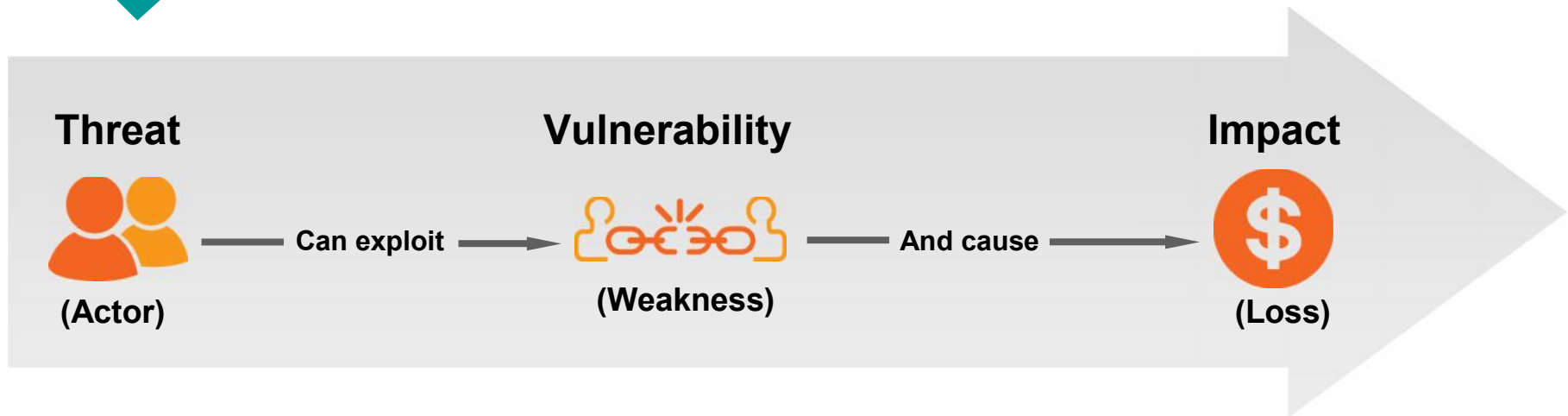
- Hactivist or other adversary launches concurrent attacks from multiple worldwide locations
- Attacks intended to saturate network connections and disable web presence
- Results in lost business opportunities and brand impact



<sup>1</sup>Distributed denial of service (DDoS)

To stay ahead we focus on disrupting the attackers capability, timeline and impact

Security risk exists when ...



**Security Risk Management** is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.



# Security essentials for chief information officers (CIOs)

IBM developed ten essential practices required to achieve better security intelligence.

### Essential practices

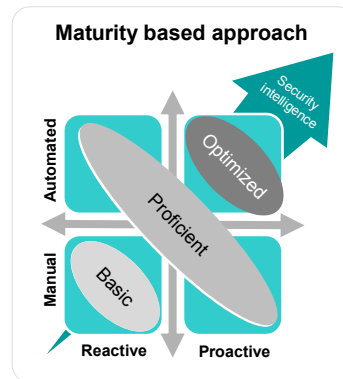
1. Build a risk-aware culture and management system

6. Control network access and help assure resilience

2. Manage security incidents with greater intelligence

7. Address new complexity of cloud and 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



## Essential practice 1: Build a risk-aware culture and management system.



### **Does your company culture enforce and track the right risk adverse behaviors?**

In using technology, everyone within a company has the potential to infect the enterprise, whether it's from clicking a dubious attachment or failing to install a security patch on a smart phone.

Building a risk-aware culture involves setting out the risks and goals, and spreading the word about them.

Management needs to push this change relentlessly from the top down, while also implementing tools to track progress.

### **Actions to help get you there:**

- Expand the mission of enterprise security from IT shop to managing IT risk across the company, driven by a leader with a strategic, enterprise-wide purview .
- Design an organization structure and governance model that enables more proactive identification and management of risks.
- Communicate and educate to raise awareness of potential cyber risks.
- Build a management system enabled by digestible policies, measurements and appropriate tools.

### **IBM Offerings**

- Governance and organizational design
- Risk management assessment and program development
- Security metrics assessment and definition
- Policy development
- Security awareness program
- Chief information security officer (CISO) on demand
- Enterprise security architecture design





## Essential practice 2: Manage security incidents with greater intelligence



### How can you use security intelligence to benefit your business?

Imagine that two similar security incidents take place, one in Brazil and the other in Pittsburgh. They may be related. But without the security intelligence to link them, an important pattern could go unnoticed.

A company-wide effort to implement intelligent analytics and automated response capabilities is essential.

Creating an automated and unified system enables an enterprise to better monitor its operations — and respond more quickly.

### Actions to help get you there:

- Build a skilled incident management and response team with sufficient resources to conduct the forensics required.
- Develop a unified incident handling policy and process.
- Leverage consistent tools and security intelligence for incident management and investigative forensics.

### IBM Offerings

- Incident response program development
- Emergency response services
- Forensics solution implementation
- Security Information and event management (SIEM)
- IBM X-Force® Threat Analysis Service



## Essential practice 3: Defend the mobile and social workplace.



### What should you consider when securing your workplace?

Employees bring growing numbers of their own devices to work and increasingly leverage social media in their communications. Each work station, laptop, or smart phone provides a potential opening for malicious attacks.

Settings on devices cannot be left to individuals or autonomous groups, but instead must be subject to centralized management and enforcement.

Securing the workforce means finding the right balance between openness and risk management.

### Actions to help get you there:

- Enable employees to bring their own devices and leverage use of social media while providing them the capabilities to segment business and personal data and protect the enterprise's data assets.
- Secure end-user computing platform to fit a risk profile based on an employee's role.
- Automate endpoint security settings enforcement across workstations, mobile devices and desktop cloud images.
- Isolate business, client and personal data and protect it.

### IBM Offerings

- Mobile and endpoint assessment and strategy
- Endpoint and server solution implementation
- Mobile device security management



## Essential practice 4: Security-rich services, by design.



### What does “secure by design” mean to my business?

Imagine if automobile companies manufactured their cars without seat belts or airbags, and then added them later. It would be both senseless and outrageously expensive.

In much the same way, one of the biggest vulnerabilities in information systems comes from implementing services first, then adding on security as an afterthought.

The best solution is to build in security from the beginning, and carry out regular automated tests to track compliance.

### Actions to help get you there:

- Assess where your optimal points of quality inspection should be.
- Reduce the cost of delivering secure solutions by embedding security in the design process.
- Use tools to scale adoption and to track compliance.
- Proactively uncover vulnerabilities and weaknesses through ethical hacking and penetration testing.

### IBM Offerings

- Security-rich engineering design and development
- Penetration testing
- Application source code assessment
- Hosted application security management
- Hosted vulnerability management





## Essential practice 5: Automate security “hygiene.”



### What are the risks of continuous patching and the use of legacy software?

People stick with old software programs because they know them, and they are comfortable with them. But managing updates on a variety of software can be next to impossible.

With a hygienic, security-rich system, administrators can keep track of every program that is running and be confident that it is current, and can have a comprehensive system in place to install updates and patches as they are released.

This “hygiene” process should be routine and embedded in the foundation of systems administration.

### Actions to help get you there:

- Register all IT infrastructure components in a centralized inventory and aggressively retire legacy components.
- Integrate compliance data for end-to-end visibility.
- Automate patch management and encourage a culture of diligence to help ensure that the infrastructure will protect against the current threats.
- Identify opportunities to outsource routine monitoring functions.

### IBM Offerings

- Infrastructure health assessment and outsourcing
- Endpoint and server solution implementation
- Hosted vulnerability management



## Essential practice 6: Control network access and help assure resilience.



### How can managed services help me strengthen controls for network access?

Imagine the IT infrastructure of a company as a giant hotel with over 65,000 doors and windows. While the public is allowed to enter through the lobby, guest room access would be controlled by registration and guest keys.

The same is true of data. Network security tools provide organizations with a way to control access to the “rooms” where confidential data and critical systems are stored..

### Actions to help get you there:

- Optimize existing investments and leverage new technologies to monitor and protect against threats.
- Detect and block malicious network activity using a combination of logging, monitoring and advanced analytics solutions.
- Prioritize what you need to control and what you do not need to control.
- Optimize network infrastructure to improve both performance and risk management.

### IBM Offerings

- Network security assessment
- Managed intrusion detection system and intrusion protection system (IDP and IPS)
- Managed firewall
- Managed secure web gateway
- Managed unified threat management (UTM)
- Hosted email and web security
- Security Information and event management (SIEM)
- Secure log management





## Essential practice 7: Address new complexity of cloud and virtualization.



### How can you embrace cloud technology while reducing risk?

Cloud computing promises enormous efficiencies. But it can come with some risk. If an enterprise is migrating certain IT services to a cloud computing, it will be in close quarters with lots of others—possibly including individuals who may have malicious intent.

To thrive in this environment, organizations must have the tools and procedures to isolate and protect themselves, and to monitor potential threats.

### Actions to help get you there:

- Develop a strategy for better securing your own cloud services.
- Assess the security controls of other cloud providers to protect your data.
- Understand the strengths and vulnerabilities of your cloud architecture, programs, policies and practices.
- Build cloud services that employ a higher level of control and confidence.

### IBM Offerings

- Cloud security strategy and assessment
- Hosted vulnerability management
- Hosted application security management
- Managed firewall
- Managed intrusion prevention and detection systems (IPDS)
- Security information and event management (SIEM)
- Secure log management



## Essential practice 8: Manage third-party security compliance.



### Are your security policies and safeguards compliant today?

An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers.

Security, like excellence, should be infused in the entire partner ecosystem. Numerous cases have shown how the carelessness of one company can have a deleterious effect on many.

### Actions to help get you there:

- Integrate security as a part of mergers and acquisitions.
- Assess vendors' security and risk policies and practices, and educate them on compliance.
- Assess conformance with process and data protection requirements of industry requirements and regulations such as PCI<sup>1</sup>, GLBA<sup>2</sup>, HIPAA<sup>3</sup>, SOX<sup>4</sup>, NERC-CIP<sup>5</sup>.
- Manage the vendor risk lifecycle.

### IBM Offerings

- Third-party compliance assessment
- PCI<sup>1</sup>, GLBA<sup>2</sup>, HIPAA<sup>3</sup>, SOX<sup>4</sup>, NERC-CIP<sup>5</sup>



<sup>1</sup>Payment card industry (PCI), <sup>2</sup>Gramm-Leach-Bliley Act (GLBA), <sup>3</sup>Health Insurance Portability and Accountability Act (HIPAA), <sup>4</sup>Sarbanes-Oxley (SOX),  
<sup>5</sup>North American Electric Reliability Corporation-Critical Infrastructure Protection (N ERC-CIP)

## Essential practice 9: Better secure data and protect privacy.



### How can you improve the protection of your critical data?

Every company has critical information, Perhaps its scientific and technical data, or maybe its documents regarding possible mergers and acquisitions, or clients' non-public financial information.

Each enterprise should carry out an inventory, with the critical data getting special treatment. Each priority item should be guarded, tracked and encrypted as if the company's survival hinged on it. In some cases, that may be the case.

### Actions to help get you there:

- Identify the value of your confidential data and the business impact of loss.
- Assess gaps and define a data protection strategy that manages data loss risk and meets governmental and customer requirements.
- Design a robust data management architecture that protects your sensitive or confidential information.
- Deploy and manage leading data protection technologies.

### IBM Offerings

- Data security and privacy strategy and assessment
- Data loss prevention
- Data encryption
- Database security assessment and architecture
- Big Data security architecture
- Database auditing and monitoring
- Data masking







## Essential practice 10: Manage the identity lifecycle.



### What value does managing the identity and access of users bring to my business?

Managing who has access to critical data is essential element of security. For example, imagine that a contractor gets hired full time. Six months pass and he or she gets a promotion. A year later, a competitor hires him or her. How does the system treat that person over time?

It must first give limited access to data, then open more doors before finally denying access to him or her.

This is managing the identity life cycle. It's vital. Companies that mismanage it are operating without enough information, and could be vulnerable to intrusions.

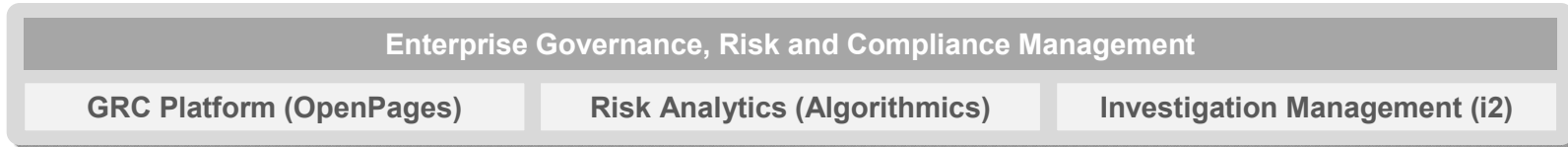
### Actions to help get you there:

- Develop an optimized identity and access management strategy.
- Implement standard, policy based control mechanisms and more intelligent monitoring.
- Centralize and automate separation of duties management.
- Adopt a desktop and web single-sign-on solution.

### IBM Offerings

- Identity management assessment and strategy
- Identity solution Implementation
- Role analytics
- Two-factor authentication
- Public key infrastructure (PKI) deployment





**IBM Security Portfolio**

**Security Intelligence, Analytics, and Governance, Risk, and Compliance**

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager
Risk and Awareness Services	3 <sup>rd</sup> Party and Regulatory Compliance	Managed and Cloud-based SIEM

**Operational IT Security Domains and Capabilities**

People	Data	Applications	Network	Infrastructure	Endpoint
Identity and Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard and Source	Network Intrusion Prevention	Endpoint Manager (BigFix)	
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization and Server Security	
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Network Anomaly Detection	Mainframe Security (zSecure, RACF)	
Identity Strategy & Assessment	Data Strategy & Architecture	Secure Engineering	Managed Firewall, Intrusion Prevention, UTM Services	Incident Response	
Identity Solution Implementation	Encryption and DLP Solution Implementation	Dynamic and Source Code Application Testing	Vulnerability Mgmt, Web & Email Security	Mobile Security Strategy & Mgmt	

Security Consulting

Managed and Cloud Services

X-Force and IBM Research

v12-12

Products [Services](#)



## IBM is helping to solve essential security challenges—worldwide.



### Better secure data and protect privacy

A large Canadian pharmaceutical company improves its ability to protect against internal and external threats with an IBM Information Security Assessment



### Control network access and help assure resilience

A Danish dairy company protects users and its infrastructure from malicious content and limits administration



### Defend mobile and social workplace

A leading manufacturer in India identifies potential security threats, strengthens its security levels and improves customer confidence



### Manage third-party security compliance

A US Retailer identifies gaps to achieve Payment Card Industry (PCI) compliance



### Address new complexity of cloud and virtualization

An urban services organization in Portugal, improves employee productivity through e-mail filtering and cloud/managed security services



### Security-rich services by design

A bank in Kuwait gains a better view of its security posture and network vulnerabilities by conducting real-world security testing



### Build a risk-aware culture

An Austrian bank conglomerate establishes a consistent security policy with IBM Security Services



# Why IBM ?



IBM can provide unmatched global coverage and security awareness.



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

## IBM Research



**10B** analyzed web pages and images  
**150M** intrusion attempts daily  
**40M** spam and phishing attacks  
**46K** documented vulnerabilities and millions of unique malware samples



**Worldwide managed security services coverage**

- 20,000-plus devices under contract
- 3,300 GTS<sup>1</sup> service delivery experts
- 3,700-plus MSS<sup>2</sup> clients worldwide
- 15B-plus events managed per day
- 3,000-plus security patents
- 133 monitored countries (MSS)

<sup>1</sup>IBM Global Technology Services (GTS); <sup>2</sup>Managed Security Services (MSS)

We continue to research, test and publish focused approaches to IT security that align with both executive and technical needs.

Finding a Strategic Voice  
[IBM 2012 CISO Assessment](#)



IBM Institute for Advanced Security  
[Global Security Leaders Share intelligence and collaborate](#)



IBM 2012 Global Chief Executive Officer Study  
[Security Intelligence and Compliance Analytics](#)



Thank you for your time today.

**For more information:**

[IBM Security Services](#)

[CIO Secure and Resilient Enterprise](#)

[Managing Risk, Security and Resiliency](#)

**Contact:**

- Stewart Cawthray, Chief Security Architect - IBM Security Services (Canada)
- (416) 478-3381
- [cawthray@ca.ibm.com](mailto:cawthray@ca.ibm.com)



## Trademarks and notes

IBM Corporation 2012

- IBM, the IBM logo, ibm.com and X-Force are [trademark Web site](#)], 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 the appropriate symbol (® or ™), these symbols indicate US 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: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).
- Other company, product and service names may be trademarks or service marks of others.
- The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.
- References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.
- THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.