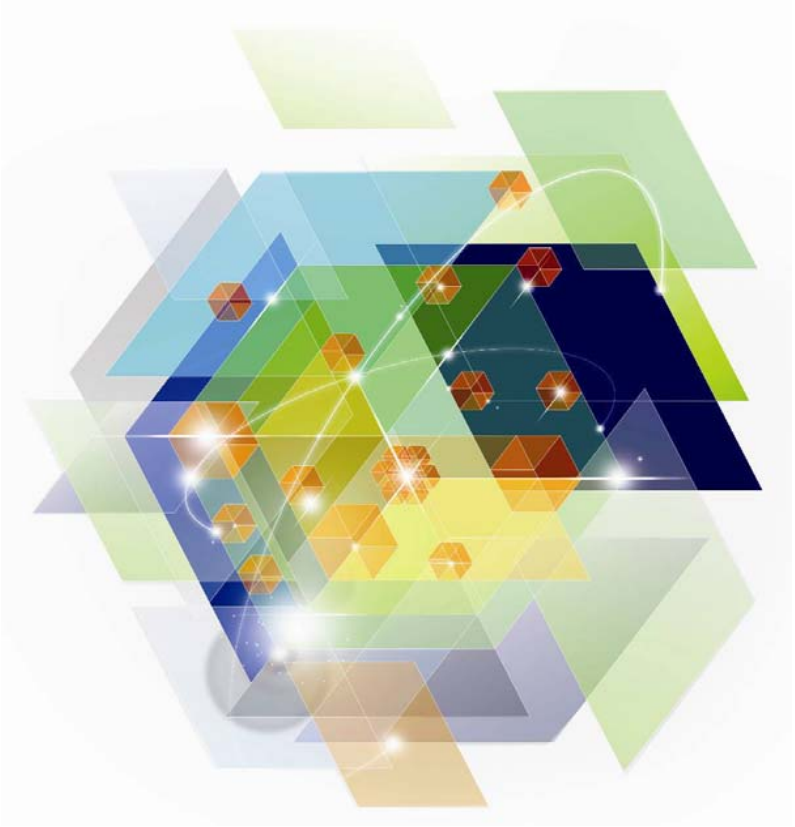
Transforming with Confidence: Balancing Risk and Innovation



IBM IT Risk Management – Our Mission

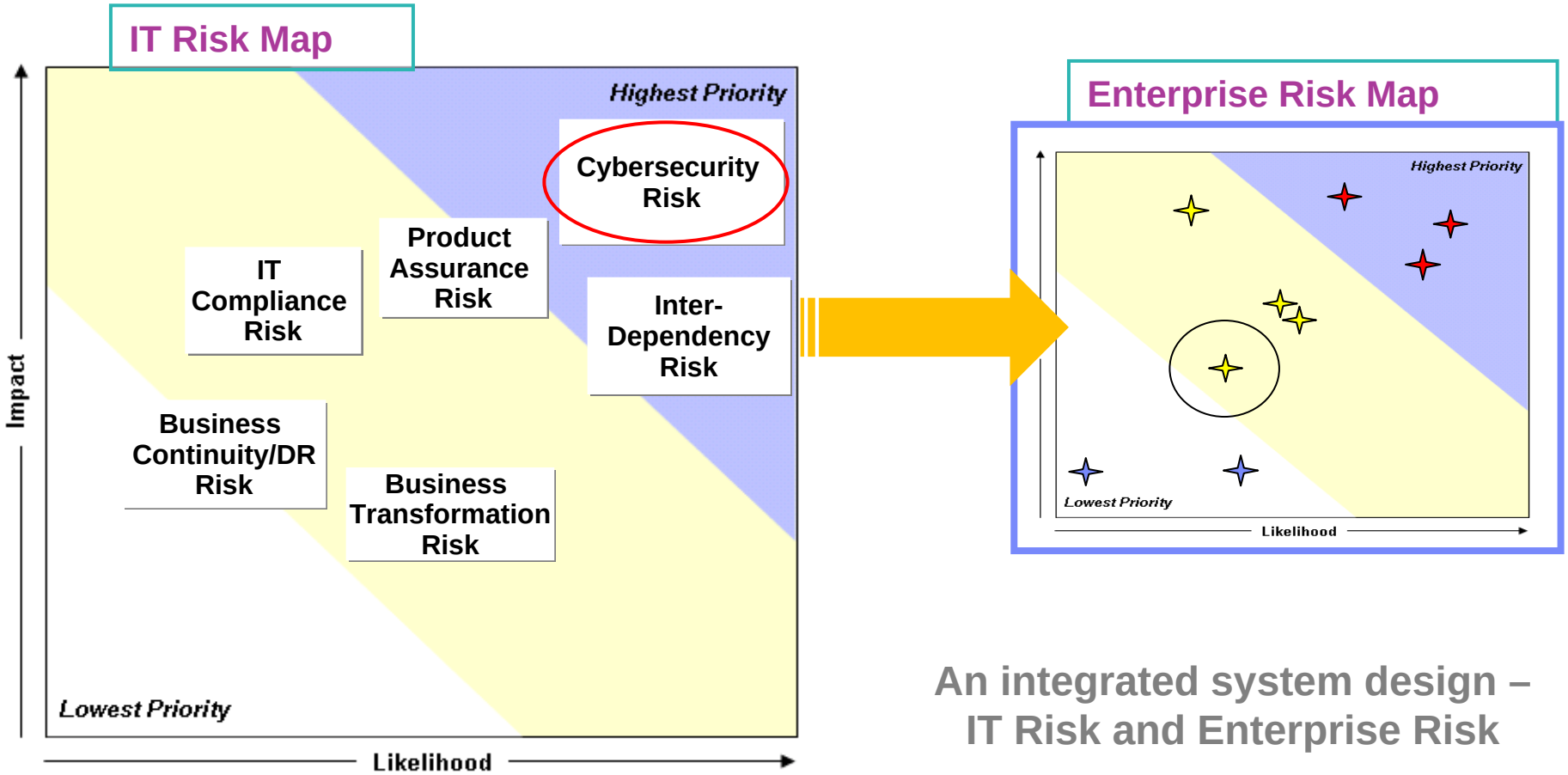
“Organizational focus & management system to define, categorize, prioritize, and make deliberate decisions regarding IT risk”

IBM IT Risk Mission – Transformation Triggers

- **The bulk of IT Risk investments were historically event-driven**
  - Crisis
  - Compliance
  - End of year (“money falls from the sky”)
- **Fragmented management system**
  - IT Security function (IT integrity)
  - Information Security function (Data confidentiality & integrity)
  - Compliance function (Application control testing)
  - Business continuity & disaster recovery function (IT availability)
  - Business transformation risk function
- **Too many dashboards, too little information**

IBM IT Risk Mission – Today's Scope

Cybersecurity Risk is assessed, managed and reported within the IT Risk Management Process and rolls up to and is reported as a Risk Category on the Enterprise Risk Map



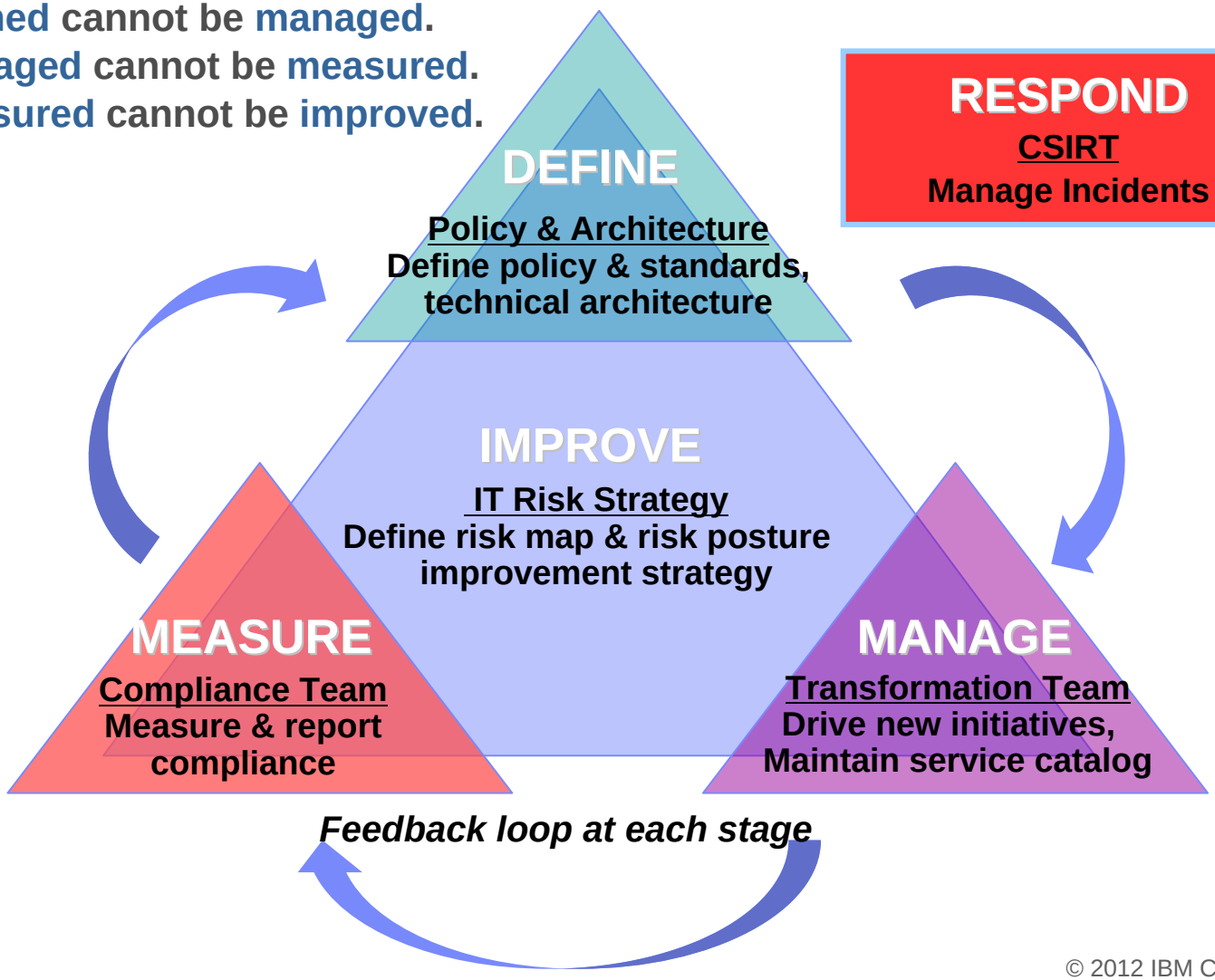
An integrated system design – IT Risk and Enterprise Risk

Note: Placement of risks is on a relative not absolute scale; Placement of risks is for the sole purpose of providing input to determine priorities

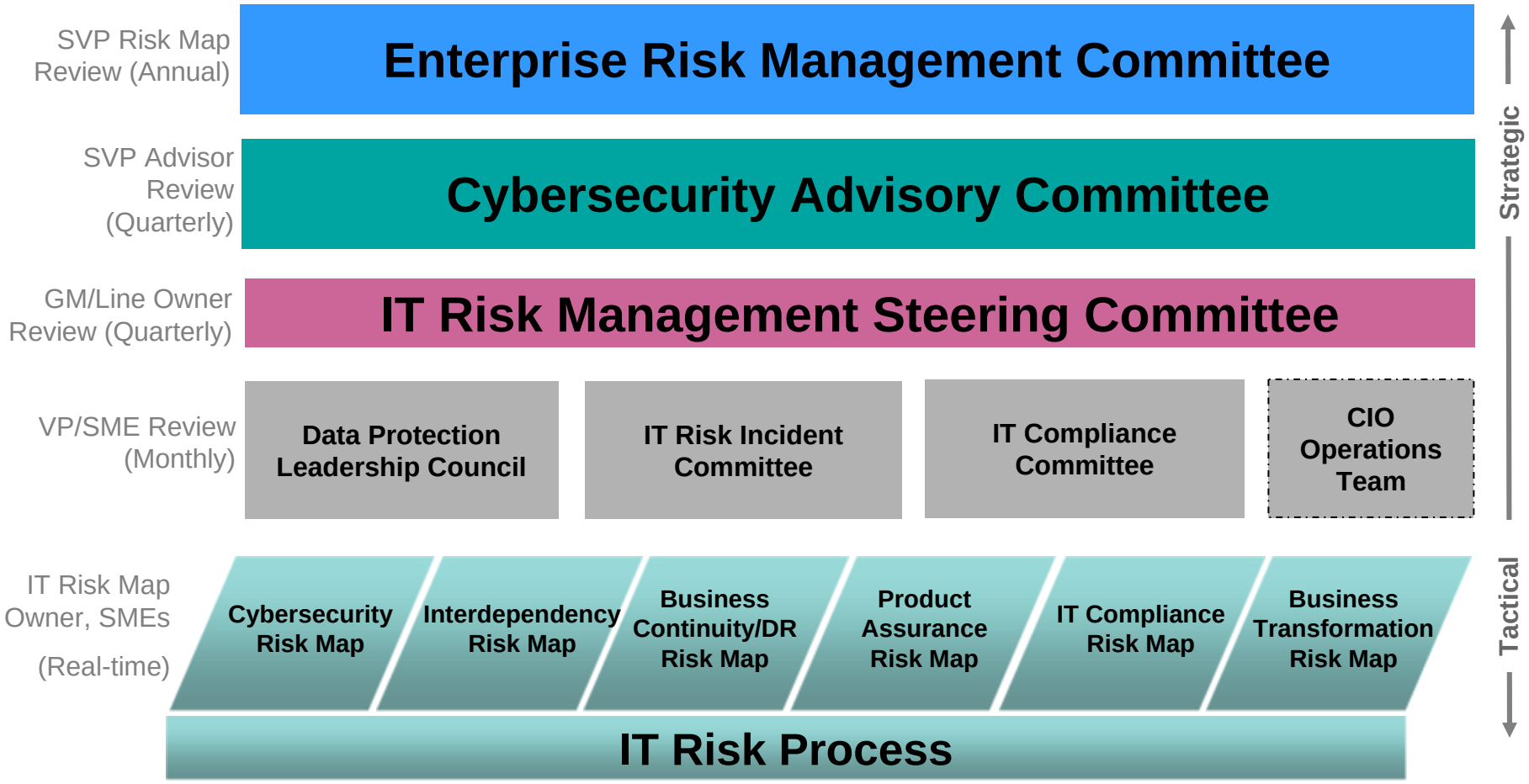
IBM IT Risk – Functional Organization

Define. Manage. Measure. Improve.

- What is not **defined** cannot be **managed**.
- What is not **managed** cannot be **measured**.
- What is not **measured** cannot be **improved**.

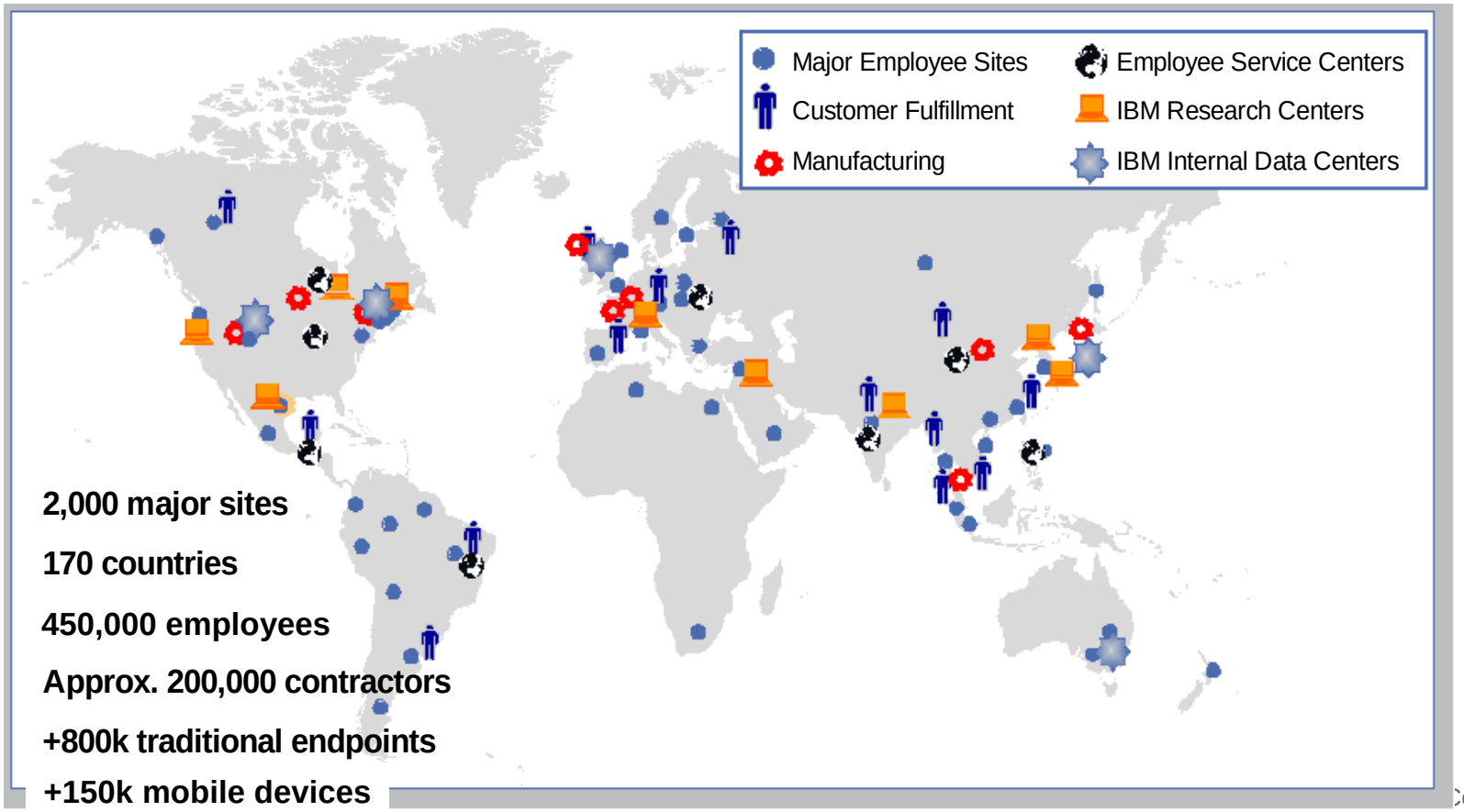


Aligning the Cybersecurity Agenda to Strategic Priorities: *Gaining Executive Consensus*



Cybersecurity Risk – Why do we worry?

Threat (Actor) — CAN EXPLOIT → **Vulnerability** (Weakness) — AND CAUSE → **Impact** (Cost)



Why do most experts believe current controls are no longer adequate to protect against cyber security attacks?

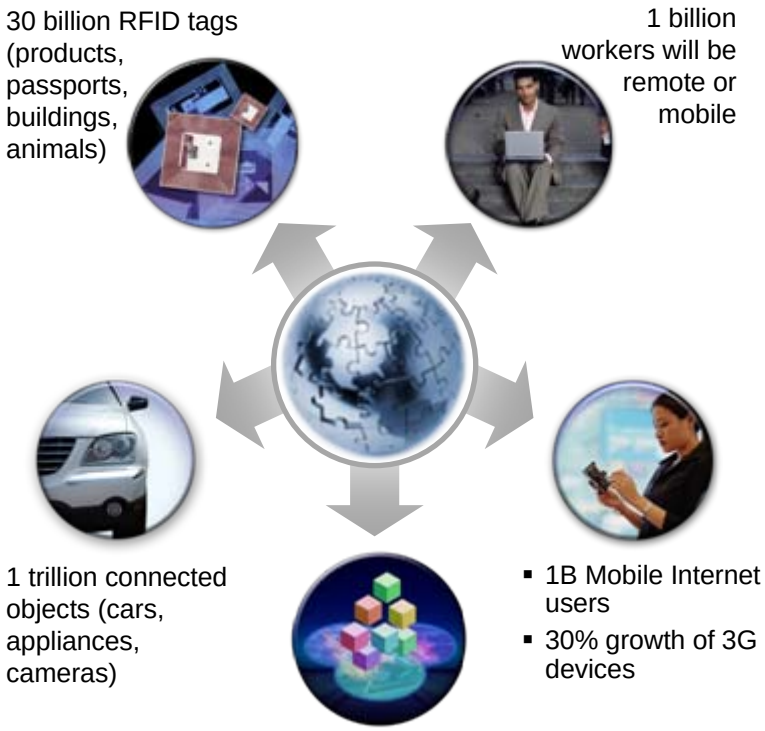
Cyber Threats (Actor) are more sophisticated

Threat Level 0	Threat Level 1	Threat Level 2	Threat Level 3
Inadvertent Actor	**Opportunist**	**Mercenary**	**Advanced Persistent Threat**
▪ Insiders - Employees, Contractors, Outsourcers	▪ Worm & Virus Writers ▪ Script Kiddies	▪ Industrial Spies ▪ Organized Crime ▪ White Hat and Black Hat Hackers	▪ National Governments ▪ Organized Crime ▪ Terrorist Cells
60%	20%	=<10%	=<10%
▪ Inexperienced ▪ No funding ▪ Causes harm inadvertently (accidentally) by unwittingly carrying viruses, or posting, sending or losing sensitive data ▪ Increasing in prevalence with new forms of mobile access	▪ Inexperienced ▪ Limited funding ▪ Opportunistic Behavior ▪ Target known vulnerabilities ▪ Use viruses, worms, rudimentary trojans, bots ▪ Acting for thrills, bragging rights ▪ Easily detected	▪ Higher-order skills ▪ Well financed ▪ Target known vulnerabilities ▪ Use malware as means to introduce more sophisticated tools ▪ Acting for profit ▪ Target and exploit valuable data ▪ Detectable, but hard to attribute ▪ Increasing in prevalence	▪ Very sophisticated tradecraft ▪ Foreign intelligence agencies, other organized crime groups ▪ Very well financed ▪ Target technology as well as information ▪ Establish covert presence on sensitive networks ▪ Difficult to detect ▪ Increasing in prevalence

Cyber Vulnerabilities increase dramatically with emergence of mobile, cloud, BYOD, Web 2.0

Embracing New Technologies, Adopting New Business Models

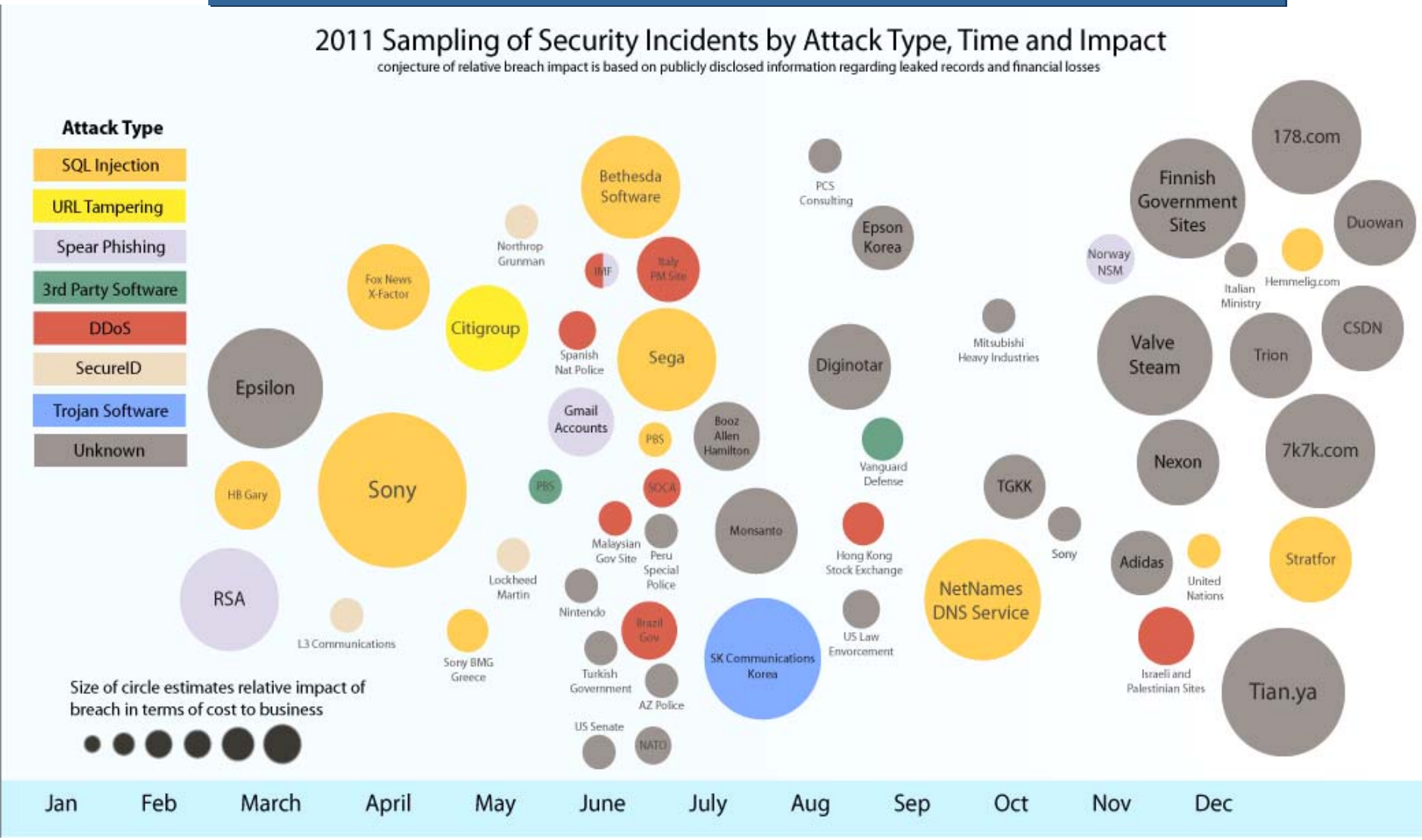
Exploding and Interconnected Digital Universe



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

Cyber Impact (Cost) increases in size, scope

Cyber security is now considered a "board level" issue…



Top Reasons Why Compromises Occur

Top 10 most exploited weaknesses end-users / endpoints

1. **Careless double-clicking**
2. **Disabling endpoint security**
3. **Using legacy hardware and software**
4. **Privileged activities from mixed-use device**
5. **Failing to install patches**
6. **Failing to install or update anti-virus**
7. **Failing to report lost or stolen device**
8. **Unsecured wireless**
9. **Weak**
10. **Giving out passwords over the phone**

Top 10 most exploited weaknesses infrastructure

1. Not hardening systems / images
2. Test systems with default passwords
3. Failing to install patches
4. Failing to install or update anti-virus
5. Using legacy/EOL hardware, software
6. Running unnecessary services
7. Using insecure management systems
8. Failing to remove old/unused accounts
9. Badly configured firewalls
10. Failing to segment network or properly monitor traffic / deploy IPS

80-90% of all security incidents can be easily avoided.

Awareness, Education, and Behavioral Change have become essential.

Build strategy based on “defense in depth”

Workforce Mobility

Supply Chain Security

Security Governance Mgmt

Incident Response

Network Security

Secure Services Engineering

Infrastructure Hygiene

Cloud and Virtualization Security

Policy & Procedures

Incident Handling & Response

Gateway Content Filtering

Vulnerability Management

Hypervisor Security

OS & Application Hardening

Authentication
Access Rights

Encryption
Data Loss Protection

Anti-Virus

Patch Management

Configuration Control

Virtual Image Management

Pen Testing/Ethical Hacking

Intrusion Detection/Prevention

Forensics

Education & Awareness

Network & Application Firewalls

Security Event Management

Risk & Compliance Management

Structured and unstruc-tured data security mgmt

Identity Lifecycle Assurance

What do we at IBM do to protect ourselves?

10 Essential Practices – cybersecurity defense in depth

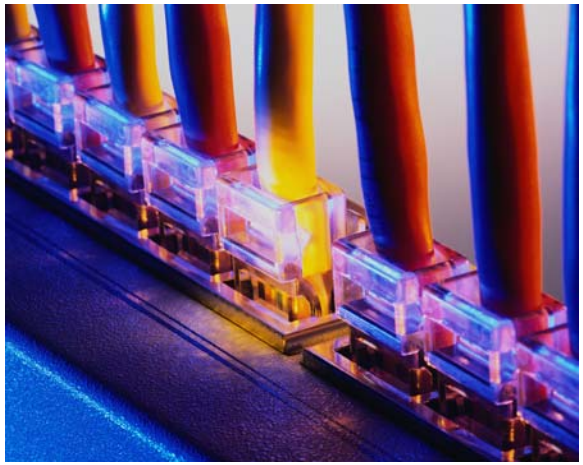
Within each essential practice, move from manual and reactive to automated and proactive to achieve optimized security.

Top Initiatives

- **Essential Practice 1: Build Risk Aware Culture & Management System**
  - Digital IBMer awareness program leveraging social media and task-based activities
  - Annual mandatory education program for all IBMers
  - Policy principles designed to maximize understanding and apply good judgment
- **Essential Practice 2: Manage Incidents & Respond**
  - Security Intelligence technology to enable real-time analysis & action
  - Forensic agents on all endpoints
- **Essential Practice 3: Defend the Workplace**
  - Hardened, virtualized workstations for all privileged users
  - Aggressive adoption of “Bring-Your-Own-Device” enabling technologies

Top Initiatives

- **Essential Practice 4: Security by Design**
  - Education and awareness programs for key development roles
  - Increased requirements for security testing within the development process, supported by on-demand vulnerability scanning
  - Increased penetration testing, application layer and network layer assessments
- **Essential Practice 5: Keep it Clean (Cybersecurity Hygiene)**
  - Block & Tackle!
  - Roll-out next generation tool for compliance health checking & reporting
- **Essential Practice 6: Control Network Access**
  - DDOS protection pre- AND post- circuit
  - Moving to cloud-based “clean pipes” model…. all connections terminate at a virtual gateway, and traffic is “cleansed” prior to reaching destination.
  - Allows for “Bring Your Own Device” strategy adoption



Top Initiatives

- **Essential Practice 7: Security in the Clouds**
  - Mandatory education for all cloud subscribers
  - 3-strike policy
  - Tools, Tools, Tools to automate humans out of security management
- **Essential Practice 8: Patrol the Neighborhood (Supply Chain)**
  - New requirements for security assessments of M&A targets during the due diligence process and immediately post announcement
  - Security policies when working with strategic vendors and suppliers
- **Essential Practice 9: Protect the Company Jewels (Structured & Unstructured Data)**
  - Expand Data Loss Protection technologies EVERYWHERE – SMTP gateways, network, endpoints, unstructured data repositories
  - Encrypt everything that can be encrypted

- **Essential Practice 10: Track Who's Who**
  - Full lifecycle identity and access management for all enterprise applications
  - Advanced technology projects (e.g. Identity Cloud pilot)

Summary

- **Take advantage of the various cybersecurity transformations**
- **Information security leaders can benefit from:**
  - **Aligning initiatives to broader, corporate-wide priorities**
  - **Articulating cybersecurity issues in the context of risk management**
  - **Shifting focus from tactical/technical to strategic/procedural**
- **Balance risk and innovation** through a pragmatic risk management and **defense-in-depth** architecture.

For more information on taking advantage of today's cybersecurity transformation, visit ibm.com/smarter/cai/security.