徐偉倫
全球科技服務部 經理
IBM Taiwan

IBM Security

「戰勝漏洞．資安預警」

企業資安成熟度評估與資安事件應變計畫

企業資安諮詢服務

內容

- 您的企業資訊真的安全嗎？ 企業資安成熟度評估

- 您的企業資訊真的安全嗎？ 企業資安事件應變計畫

您的企業資訊真的安全嗎？
企業資安成熟度評估

企業面臨持續演進的進階資安威脅，而這些新挑戰帶來業務及形象相當的風險

Business results

After its recent data breach, a retailer reported US$148M[1] in data breach-related expenses, but **executives estimate a total cost of US$1 to US2B**[2]

Brand image

The retailer also suffered major brand damage after the breach, **falling from a consistent top 10 to number 21** in the 2013 Brand Index rankings[3]

Data breach

There were 253 large-scale data breaches globally in 2013, a 62 percent rise from 2012. And eight of these **exposed more than 10 million identities each**[4]

Fraud

After stealing customer data on over 600,000 customers of a US-based company in Europe, hackers demanded ransom to not publish the information[5]

Impact of hacktivism

Anonymous Brazil, through **a series of DDoS**[6] **and web site defacement** attacks, protested the social injustice surrounding the World Cup 2014[7]

Audit risk

A major medical center and hospital were jointly **fined US$4.8M for a data breach** that compromised patient health records[8]

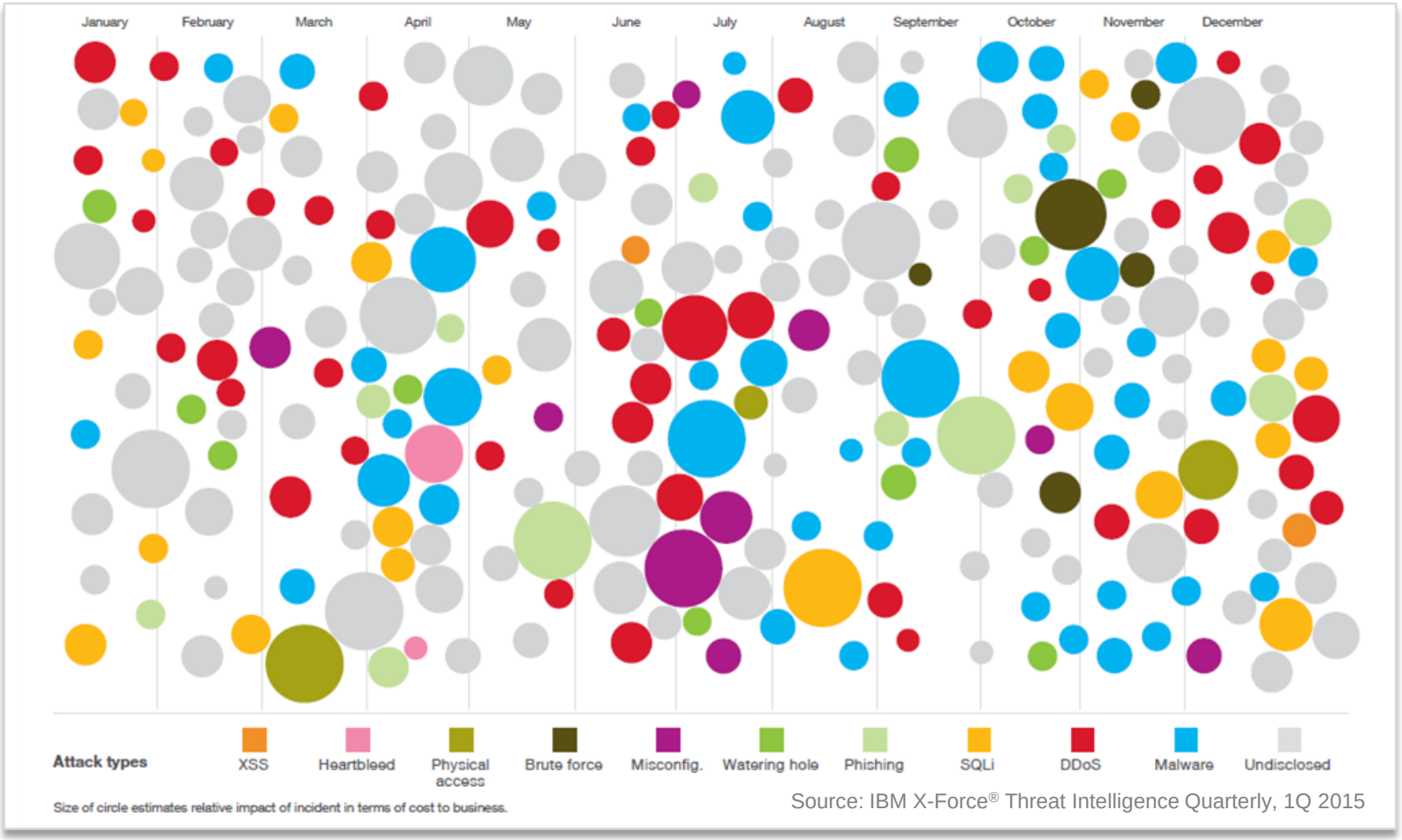
US $3.5M+ average cost of a data breach

average cost of a lost or stolen record[9] **US $201**

1) New York Times, August 5, 2014; 2) International Business Times May 5, 2014; 3) CBS MoneyWatch Jan 2014; 4) Symantec report: Latin American and Caribbean CyberSecurity Trends June 2014; 5) Reuters June 16, 2014; 6) DDoS stands for Distributed Denial of Service; 7) InfoSec Institute; Forbes, June 18, 2014; 8) McCann, Healthcare IT News, May 8, 2014; 9) Cost of Data Breach, Ponemon Institute

How do you know if your security organization is prepared to handle the next threat?

2014年機敏資料洩漏比2013年增加超過25%，企業事實上隨時處於資安風險中



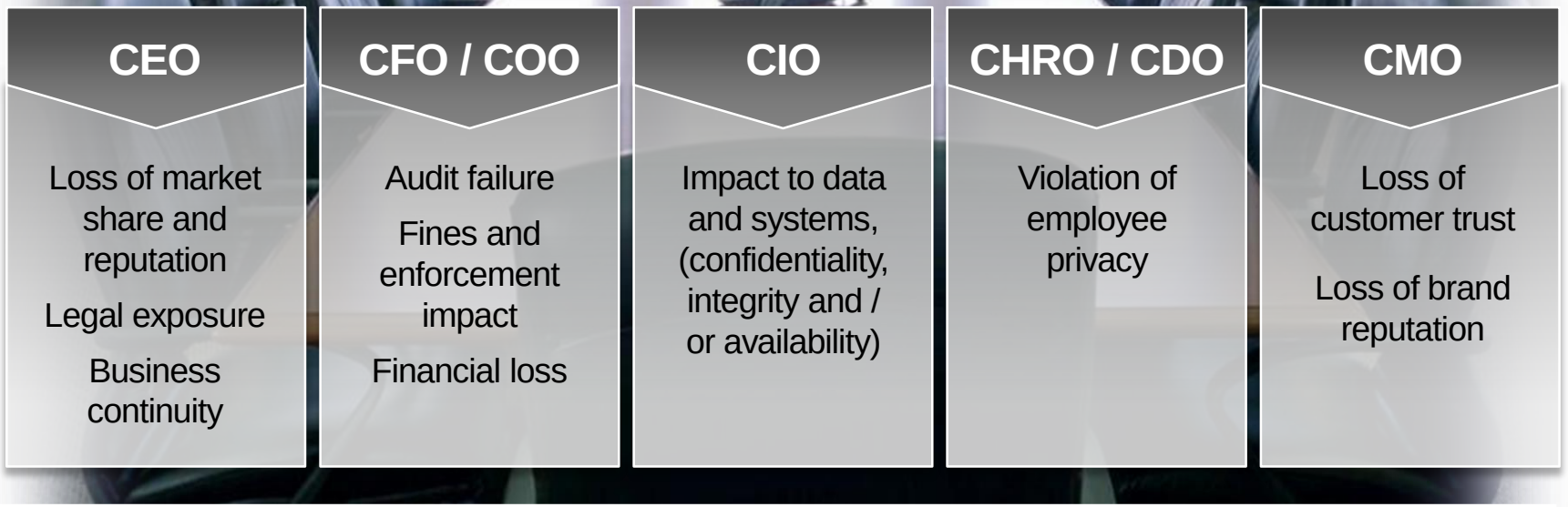
Source: IBM X-Force® Threat Intelligence Quarterly, 1Q 2015

$5.85M average cost of a U.S. data breach

$201 average cost per compromised U.S. record

Source: 2014 'Cost of Data Breach Study: Global Analysis', Ponemon Institute

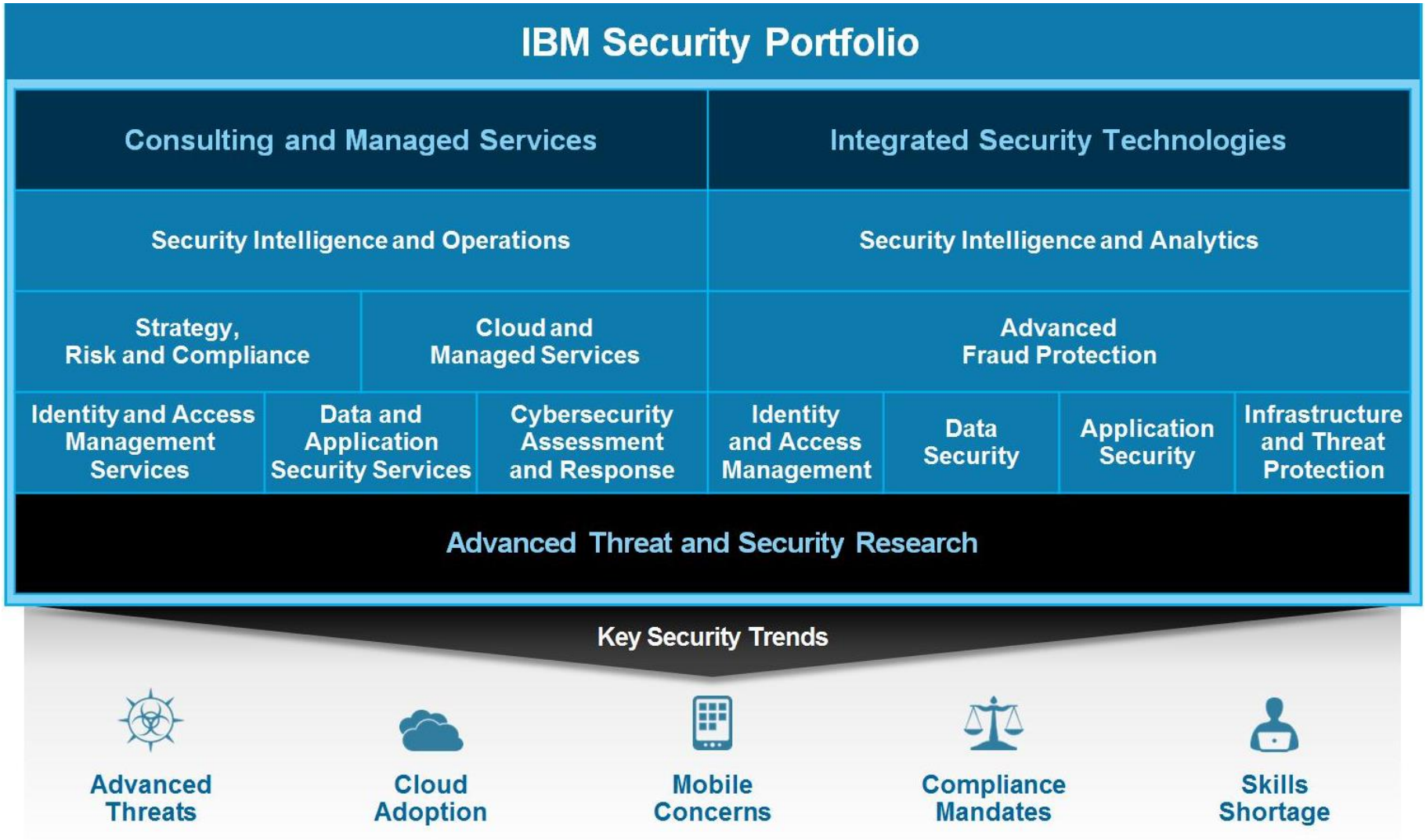
即使在不同高階主管的角色，比起過去都需負更多的企業資安責任



CEO	CFO / COO	CIO	CHRO / CDO	CMO
Loss of market share and reputation Legal exposure Business continuity	Audit failure Fines and enforcement impact Financial loss	Impact to data and systems, (confidentiality, integrity and / or availability)	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Your board and CEO demand a strategy

IBM從諮詢管理服務與整合資安技術提供企業資安的實施參考



企業可以由IBM資安服務涵蓋的資安核心基礎對整合資安框架有一完整藍圖

IBM Security Services Portfolio

Strategy, Risk & Compliance				
Security Maturity Benchmarking	Security Strategy & Roadmap Development	Security Risk Assessment & Program Design	Industrial Controls (NIST, SCADA)	PCI Advisory
Cybersecurity Assessment & Response				
Threat Intelligence Advisory	X-Force Threat Analysis	Penetration Testing	Incident Preparation	Emergency Response
Security Intelligence and Operations Consulting				
Security Intelligence Operations Center Design & Build Out Services				

Identity	Data	Applications	Infrastructure
Identity Assessment & Strategy	Crown Jewels Discovery & Protection	SDLC Program Development	Security Optimization
User Provisioning/Access Mgmt	Database Security	Dynamic and Static Testing	Design, Deployment & Migration
Total Authentication Solution	Encryption and Data Loss Prevention	Embedded Device Testing	Staff Augmentation
Managed/Cloud Identity		Mobile Application Testing	

Cloud and Managed Services				
Firewall / Unified Threat Management	Intrusion Detection & Prevention	Web Protection & Managed DDoS	Hosted E-Mail & Web Vulnerability Mgmt	Managed SIEM & Log Management

Powered by IBM's Next Generation Threat Monitoring and Analytics Platform

企業資安要如何開始加強及提升? 應從了解、評估、行動三要務著手因應威脅並保護業務

1

Understand security essentials

了解

2

Assess security maturity

評估

3

Determine critical gaps and prioritize actions

行動

在了解方面，IBM根據企業經驗總結十項核心基礎實踐(10 essential practices)來檢視企業資安落實程度

Understand security essentials

3 Secure collaboration in social and mobile workplace

4 Develop security-rich products, by design

5 Manage IT hygienically

6 Create a security-rich and resilient network

1 Build a risk-aware culture and management system

GOAL:
Intelligent cyber threat protection and risk management

2 Establish intelligent security operations and rapid threat response

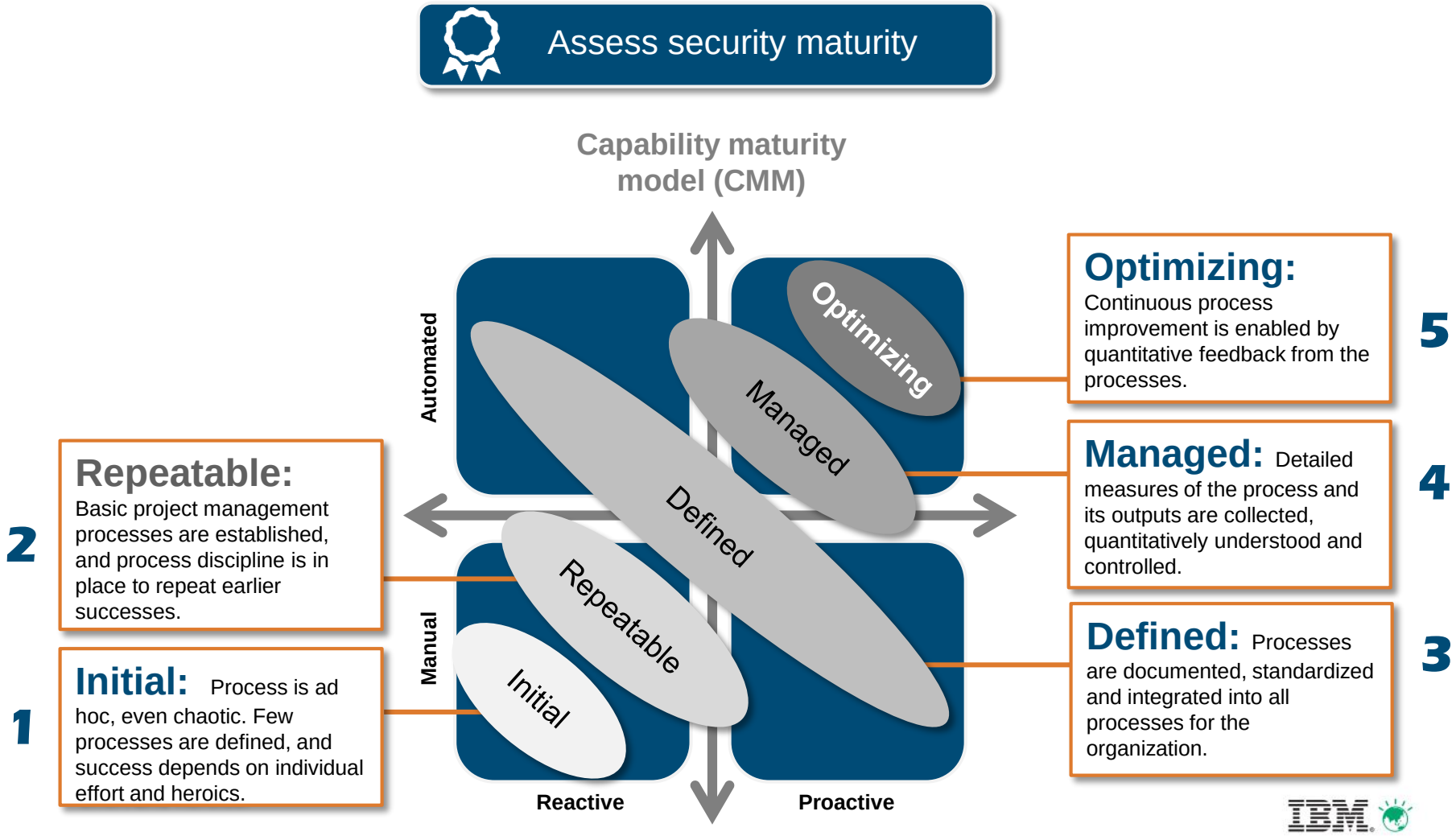
7 Address security complexity of cloud and virtualization

8 Manage third-party security compliance

9 Assure data security and privacy

10 Manage the digital identity lifecycle

接著依據成熟度模型衡量企業資安現狀與業界最佳實踐差異，來評估企業資安實施成熟度

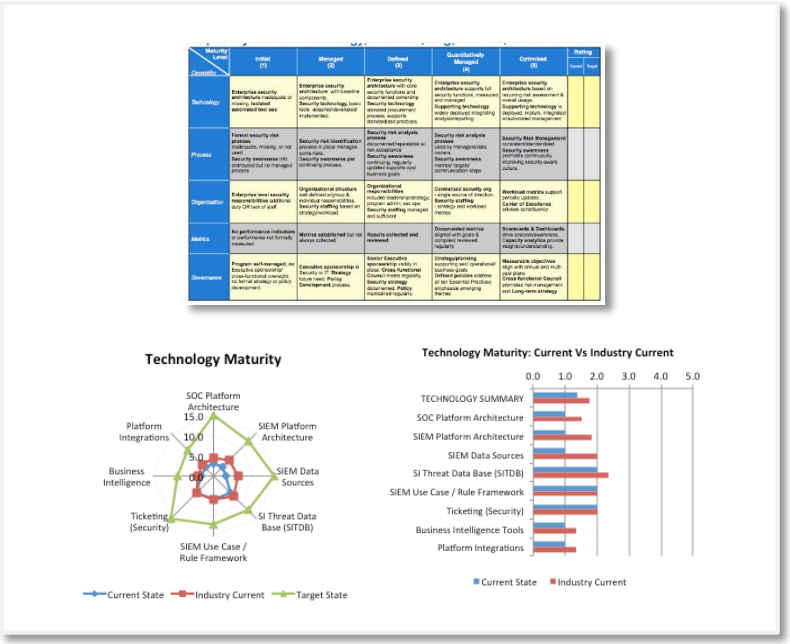


然後依照企業資安目標將優先順序條列擬訂方針，採取行動完成資安增強與提升計畫

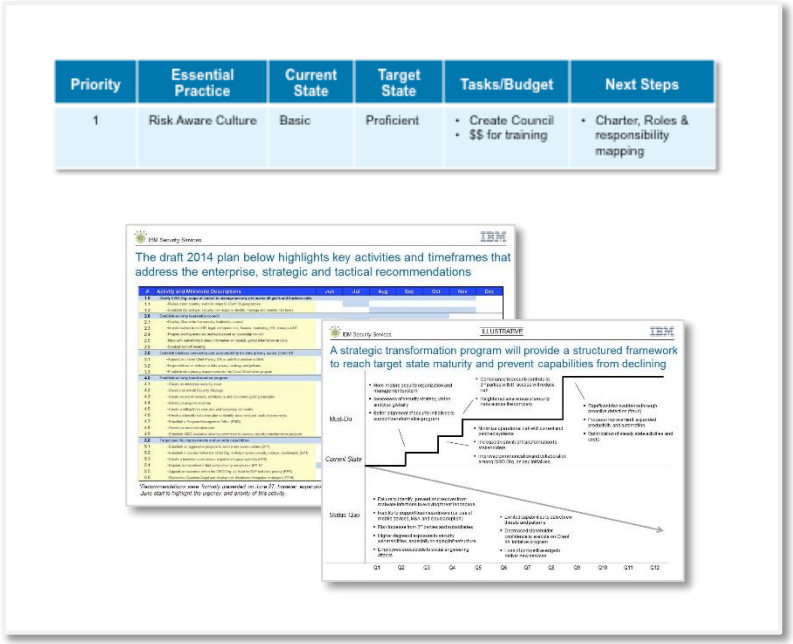
1 2 3

Determine critical gaps and prioritize actions

Security posture reviews and maturity gap analyses



Inform prioritized action plans and strategic roadmaps



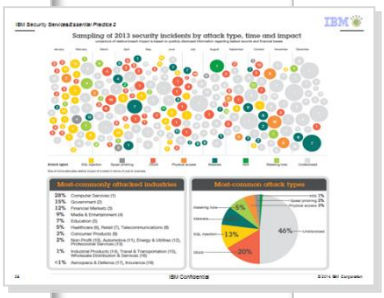
Priority	Essential Practice	Current State	Target State	Tasks/Budget	Next Steps
1	Risk Aware Culture	Basic	Proficient	• Create Council • $$ for training	• Charter, Roles & responsibility mapping

IBM提出的資安十項核心基礎實踐介紹，可以做為企業重新檢視資安的起始點

1 Essential practices presentation

Objective

- Discuss key security challenges that organizations in your industry are facing
- Provide a perspective on IBM's approach to developing a holistic security capability
- Review each of the 10 essential practices and the role each plays in a strong security posture



Details

- Typical duration of 2 to 4 hours but could go up to a full day
- Provides high-level overview as an introduction to the 10 essential practices
- Assessments and action plans are only provided in workshop or engagement

而IBM所提供的十項核心基礎實踐研討，可以進一步為企業對每一實踐評估資安薄弱環節

2 Essential practices workshop

Workshop approach

1. Review your security ecosystem	2. Assess maturity and posture across each essential practice	3. Determine and prioritize actions
▪ 10 essential practices are introduced ▪ Current understanding of a client's security ecosystem is discussed	▪ Participants discuss and align on current and target capabilities across domains ▪ Each domain is evaluated through key criteria: technology, process, people ▪ Other industry analogs are leveraged	▪ Initial prioritization of security capability gaps is conducted, with discussion of key risks ▪ Action plan is developed

Goals and outcomes

Initial alignment on your current security posture, and capabilities	Potential target maturity goals for the organization to be successful	Clarity on how capabilities are implemented through Technology, process, people, metrics and governance	Better understanding of how your security program can reduce business risk	Recommended solutions and approaches to improve*

[1]It is recommended to validate workshop conclusions before beginning implementation

另外IBM提供的十項核心基礎實踐諮詢服務，則詳細深入了解分析企業資安成熟度、比對業界最佳實踐、並提出策略藍圖及提升資安計畫

3 **Essential practices engagement**

3 to 6 week essential practices engagement key phases of work

Discovery, interviews, workshops and data collections	Capability maturity review and analysis	Assessment against industry and best practices	Transformation roadmap and action plan development
			

IBM的十項核心基礎實踐可以幫助企業全面提升有效、可行的資安能力

IBM's security essentials and maturity consulting offerings

1. EP presentation
2. EP workshop
3. EP engagement

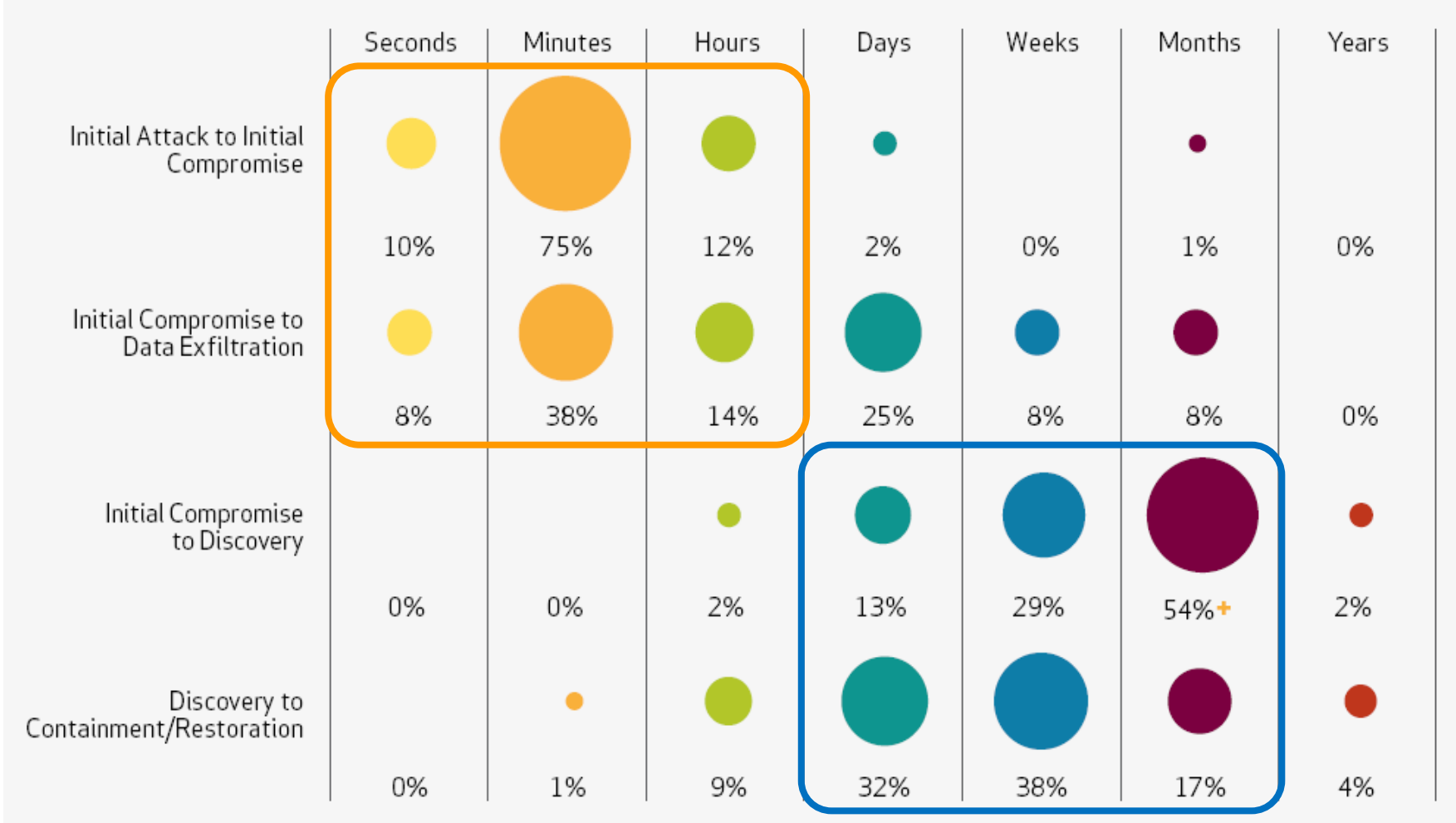
An effective and actionable security leadership capability informs critical business decisions.

您的企業資訊真的安全嗎？

企業資安事件應變計畫

Cyber Security Incident Response Plan (CSIRP)

早期偵測及快速反應是企業對資安潛伏威脅降低損害最有效的方法



Compromises take days or more to discover in 96% of cases; and over 91% weeks or more to contain

Source: Verizon Data Breach Investigations Report, 2012

所以目前資安認知及加強趨勢由”原則上安全”、”被動式保護/預防"急遽轉變為”隨時不安全”及”資安情資蒐集與反應能力”

1 Assuming a compromised environment

“One thing is clear: the longer a stealthy attacker sits undetected in the enterprise network and its endpoints, the more damage they can do.”[1]

2 Most important capabilities become intelligence and response

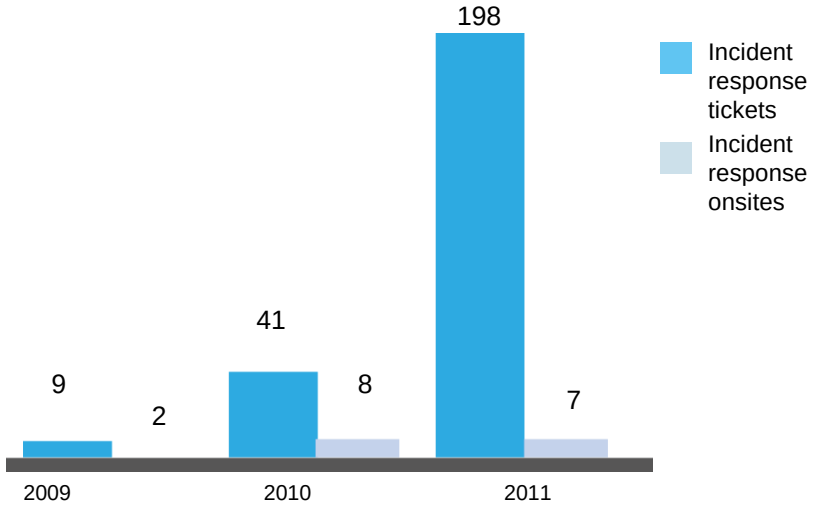
“While protection and prevention efforts should not be neglected, the true measure of an organization’s advanced persistent threat (APT) defenses is its ability to quickly detect breaches and thoroughly research the extent and impact of those breaches.”[2]

[1]Okay, Breaches Are Inevitable: So Now What Do We Do? by Paula Musich, Current Analysis, July 20, 2012, http://itcblogs.currentanalysis.com/2012/07/20/okay-breaches-are-inevitable-so-now-what-do-we-do/; [2]IBM X-Force® 2012 Mid-year Trend and Risk Report

其中提升資安事件應變能力對於進階式威脅非常關鍵

ICS- CERT incident response trends

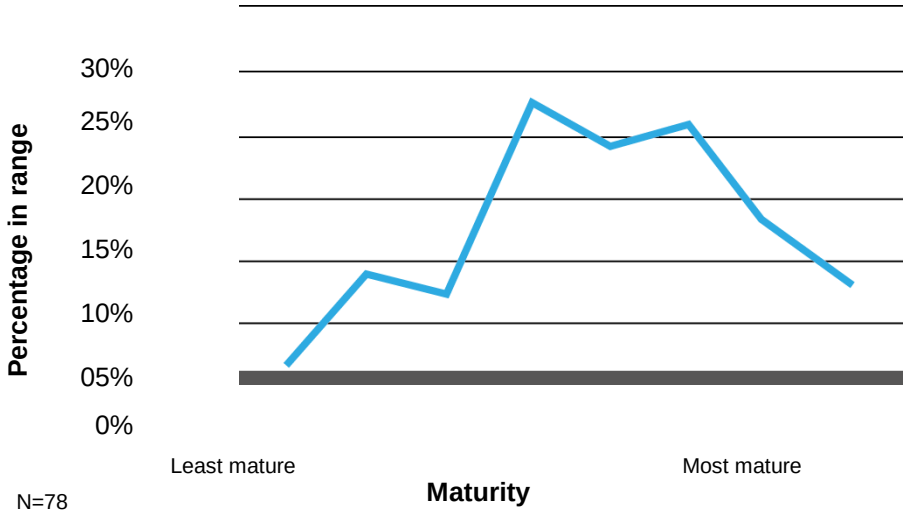
Number of attacks reported and requiring onsite
Help by US critical infrastructure companies



Source: ICS-CERT Incident Response Report. 2011

Relative maturity of IREC[1] members' incident response processes

Percentage of survey respondents at various maturity levels



Source: Information Risk Executive Council (IREC) Controls Maturity Benchmarking Service. 2009

Most organizations have outdated incident response capabilities; sophisticated attacks require chief information security officers (CISOs) to revisit their processes.

Source: 2013 Security Outlook November 2012, Information Risk Executive Council Study, Corporate Executive Board; [1]Informatoin Risk Education Council (IREC)

資安事件應變計畫服務就是為了提升企業因應資安事件作好準備

Avoid Common CSIRP[1] mistakes to build a plan that works

At least 50 percent of the CSIRPs evaluated by IBM security consultants show no evidence of a formal document lifecycle or a history of continual revisions.

Having an incident response plan in place saved U.S. organizations on average USD1.2 million per data breach in 2013.

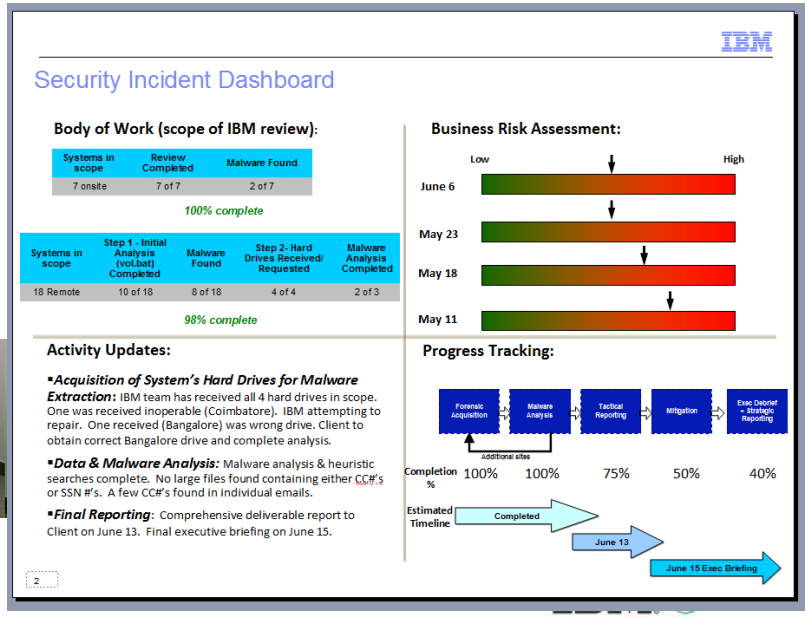
- **An incident response plan is the foundation** on which all incident response and recovery activities are based:
  - ✓ It provides a **framework** for effectively responding to any number of potential incidents
  - ✓ It specifically defines the organization, **roles and responsibilities** of the computer security incident response team (CSIRT)
  - ✓ It should have criteria to assist an organization determine **types and priorities** of each security incident
  - ✓ It defines **escalation and communication procedures** to management, executive, legal, law enforcement, and media depending on incident conditions and severity
  - ✓ It must be **regularly updated and fully tested** via dry runs

[1]CSIRP = Computer Security Incident Response Plan

資安事件應變計畫讓企業資安事件發生時，有對的流程、工具、資源來降低損失、保護關鍵資產、分析根因、回復正常、避免再次發生及法遵合規

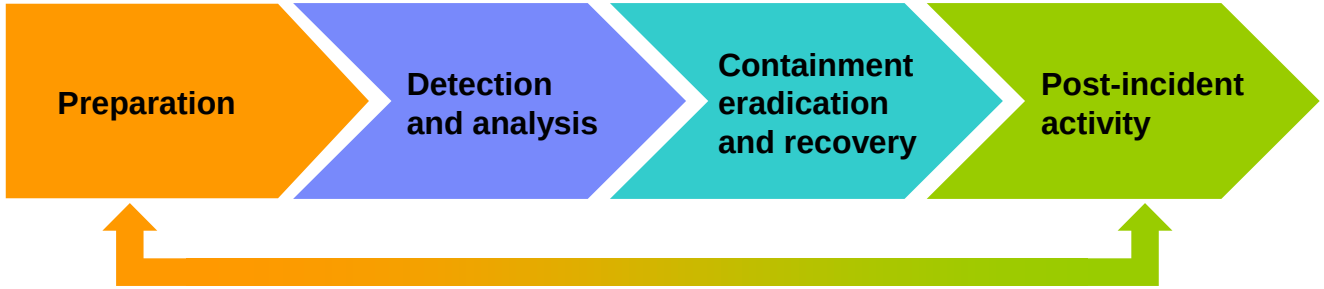
When an incident occurs, businesses need the right process, tools, and resources to respond and reduce impact.

- Being prepared to reduce the impact of a security incident and to recover faster
- Protecting critical systems and data from downtime and information theft
- Analyzing the root cause of an incident and preventing its spread
- Restoring affected systems to normal operations
- Preventing similar incidents from causing future damage
- Managing regulatory compliance requirements for incident response



企業資安事件應變計畫的框架組成需具有準備、偵測分析、排除復元、事後作為來因應任何前潛在資安事件

- The Incident response plan is the foundation on which all incident response and recovery activities are based:
  - It specifically defines the organization, roles and responsibilities of the computer security incident response team (CSIRT)
  - It should have criteria to assist an organization determine what is considered an incident versus an event
  - It defines escalation procedures to management, executive, legal, law enforcement, and media depending on incident conditions and severity
  - The plan and process should be fully tested via dry runs and incident mock tests
- A well-developed plan provides a framework for effectively responding to any number of potential security incidents



IBM具有豐富的經驗、完整的能力、成熟的方法與卓越的服務，幫助企業建立應變計畫因應任何資安事件

20 years of operations

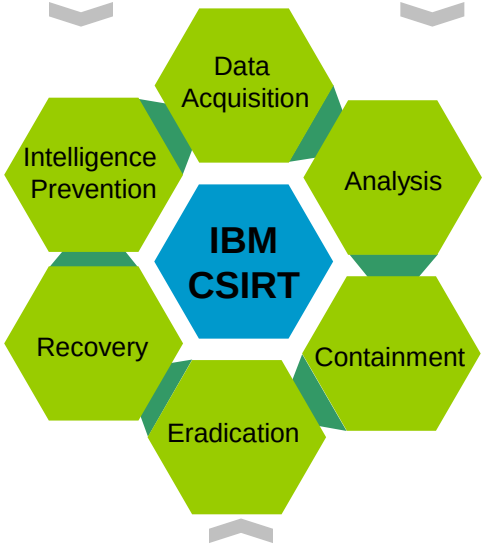
- Two decades of cybersecurity assessment and response operations that started in the US and expanded globally
- Over 260 clients in 35 countries for incidents response
- Conducts over 400 penetration tests and application assessments for over hundreds of clients worldwide

Broad capabilities

- Emergency response services
- Active threat assessment
- Cyber stress testing
- CSIRP development
- Payment card industry (PCI) forensics

Mature methodology

- Around-the-clock incident hotline
- Responds to over 500 calls every year
- Calls are answered by a skilled incident analyst
- Triage to determine if it is an event or an incident – approximately 50/50 events to incidents ratio
- Each incident is investigated and assigned severity – 60 percent of incidents are further engaged



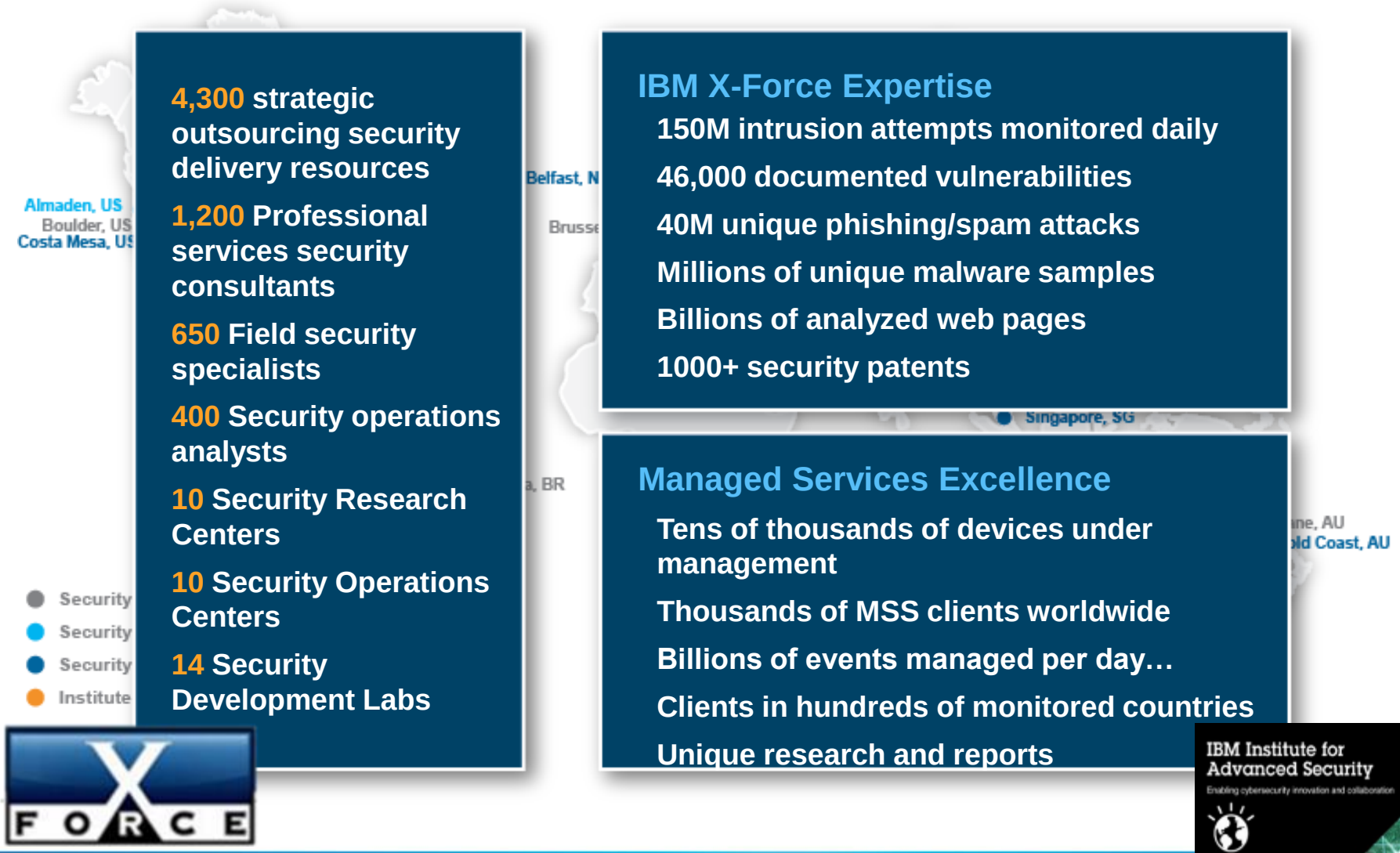
Delivery excellence

- Every project is delivered by IBMers around the globe, unless prohibited by law or special circumstances
- Each member of the CSIRT team
  - has on average 10 years of experience
  - holds multiple industry certifications
  - is equipped with US$20,000 worth of hardware, software, and forensic tools
  - gets at least US$5,000 of continued education every year

Supports IBM CIO office's internal cyber response operations

- Over 2,000 major sites
- Over 170 countries
- Over 400,000 employees
- Approximately 200,000 contractors
- Over 1 million traditional endpoints
- Around 50 percent of employees are mobile

IBM全球資源包含資安領域研究、產品發展、即時監控與分析提供完善的資安防禦與探知能力



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security