IBM Security

「戰勝漏洞．資安預警」

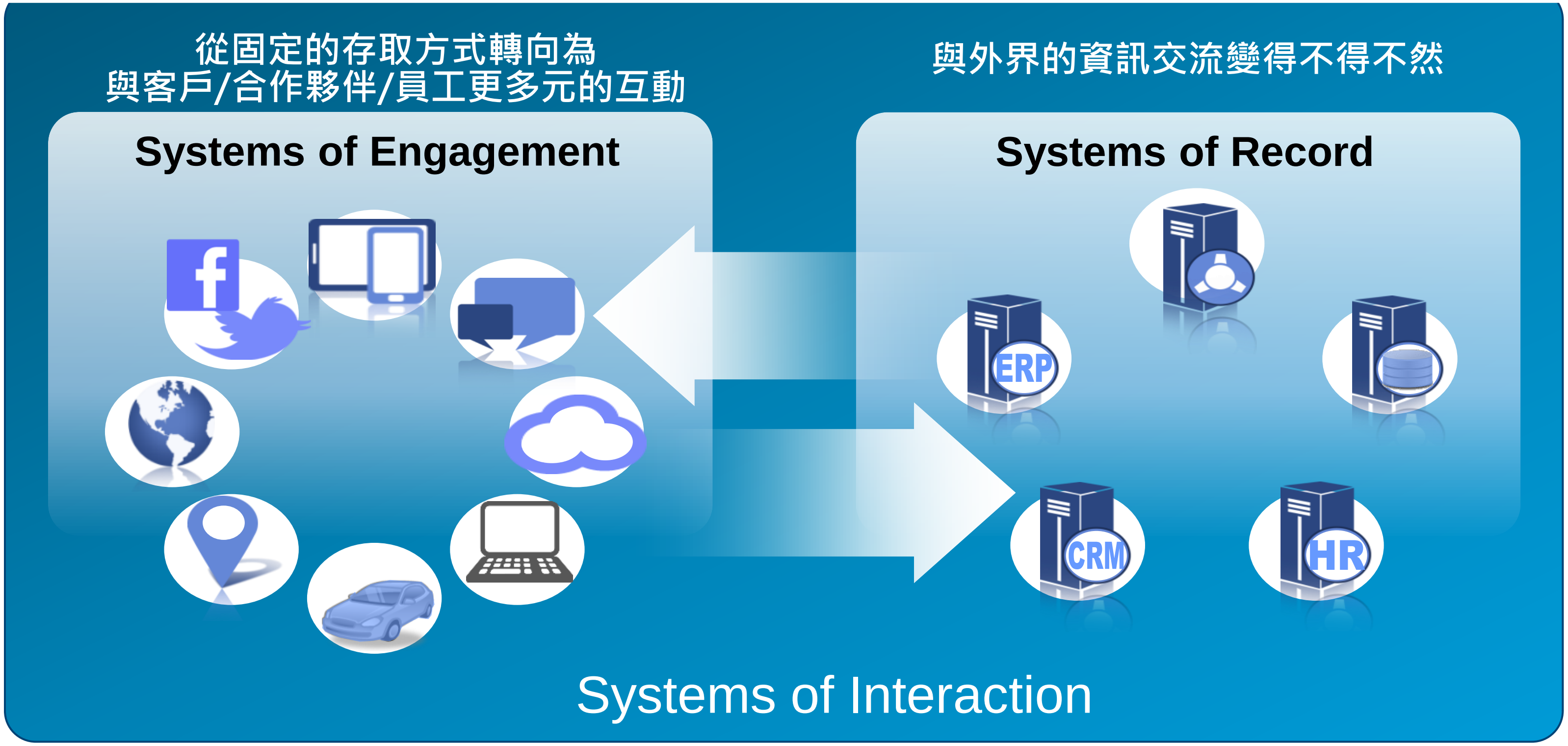
行動化變革環境下的企業安全防禦策略

IBM 全球資訊科技服務事業部 資深顧問 蔡均璋

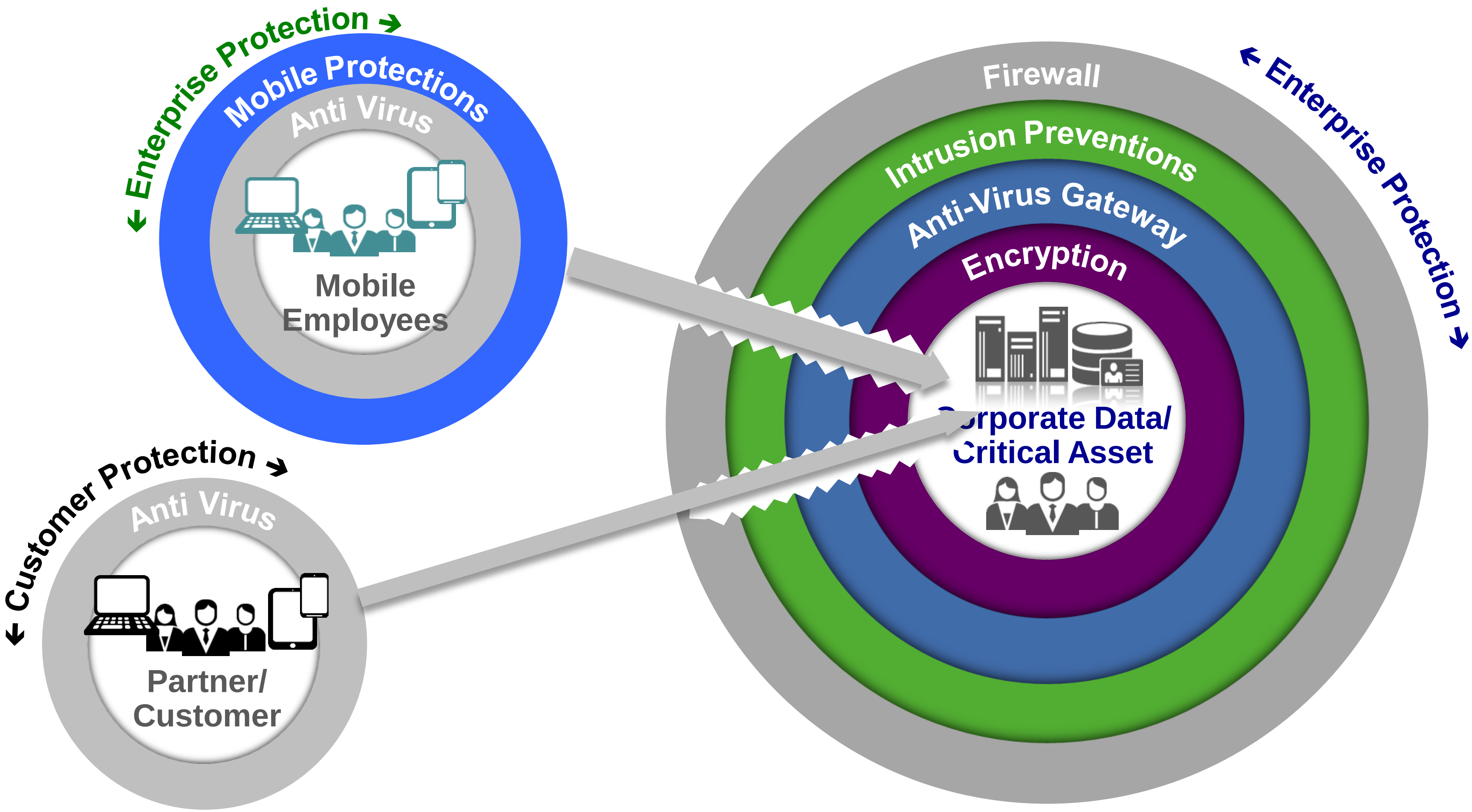
新科技與商業模式的改變
讓企業面臨開放與外界交流的壓力

業務需求

- 提昇互動模式以因應越來越高的客戶要求
- 更敏捷的處理及回應能力以提升生產力
- 建立更新的商業模式以創造新的營收來源



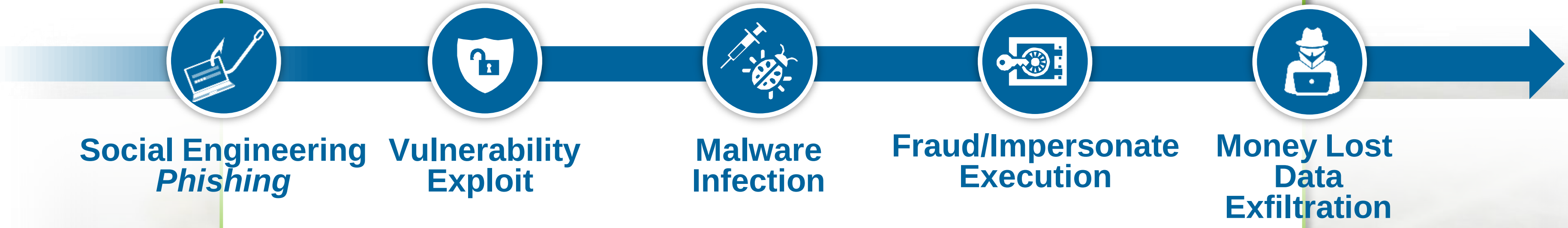
行動化的科技變革
讓傳統的企業安全防護藩籬面臨解構

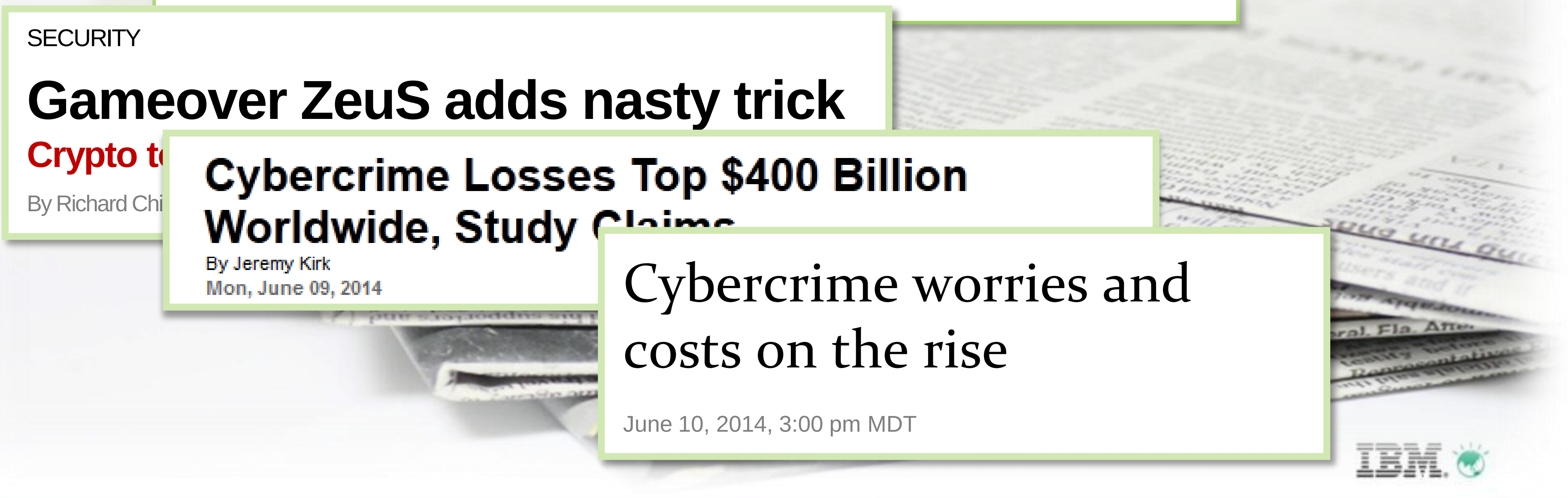


人與系統的弱點在所難免

Three Never-ending Battles

1. Humans will always make mistakes
2. System and application vulnerabilities continue to emerge
3. Malware detection will always lag





SECURITY

Gameover ZeuS adds nasty trick

Crypto t

By Richard Chi

Cybercrime Losses Top $400 Billion Worldwide, Study Claims

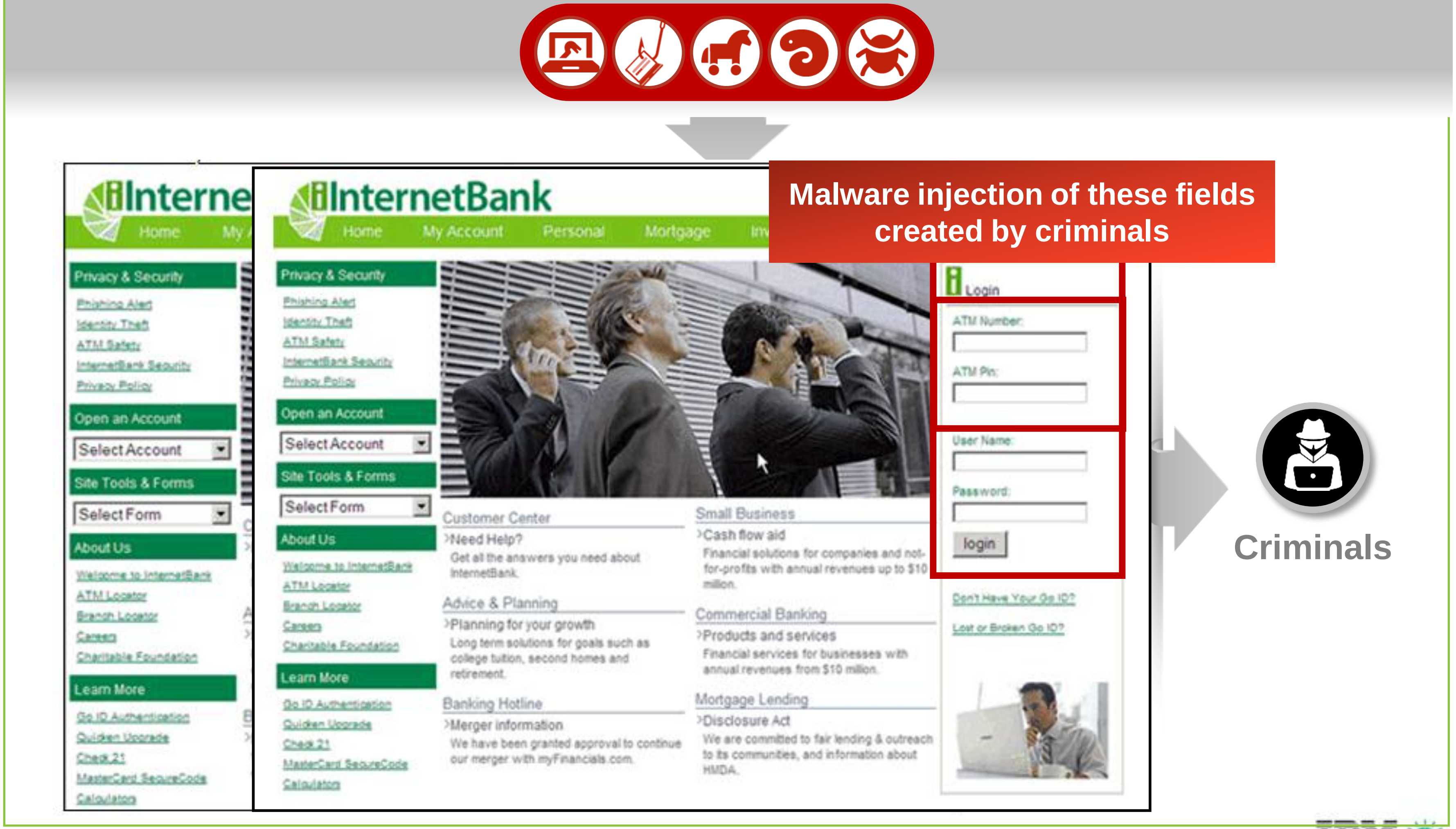
By Jeremy Kirk
Mon, June 09, 2014

Cybercrime worries and costs on the rise

June 10, 2014, 3:00 pm MDT

攻擊手法則不斷演進

Man-in-the Browser Malware



InternetBank

Customer Center

›Need Help?

Get all the answers you need about InternetBank.

Advice & Planning

›Planning for your growth

Long term solutions for goals such as college tuition, second homes and retirement.

Banking Hotline

›Merger information

We have been granted approval to continue our merger with myFinancials.com.

Small Business

›Cash flow aid

Financial solutions for companies and not-for-profits with annual revenues up to $10 million.

Commercial Banking

›Products and services

Financial services for businesses with annual revenues from $10 million.

Mortgage Lending

›Disclosure Act

We are committed to fair lending & outreach to its communities, and information about HMDA.

Login

ATM Number:

ATM Pin:

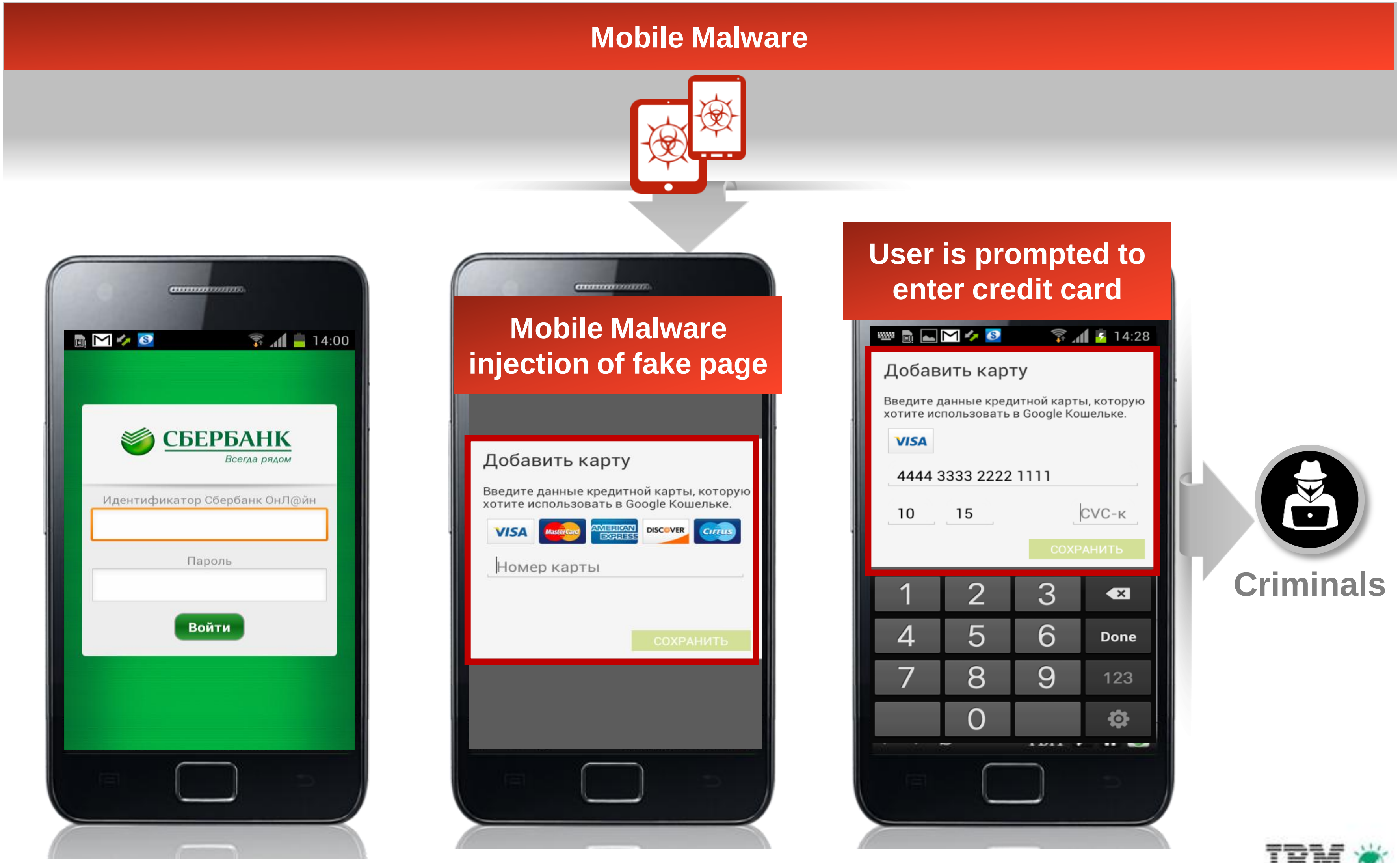
User Name:

Password:

Malware injection of these fields created by criminals

Criminals

攻擊手法則不斷演進



Mobile Malware

14:00

СБЕРБАНК

Всегда рядом

Идентификатор Сбербанк ОнЛ@йн

Пароль

Войти

Mobile Malware injection of fake page

Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

VISA MasterCard AMERICAN EXPRESS DISCOVER Cirrus

Номер карты

СОХРАНИТЬ

User is prompted to enter credit card

14:28

Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

VISA

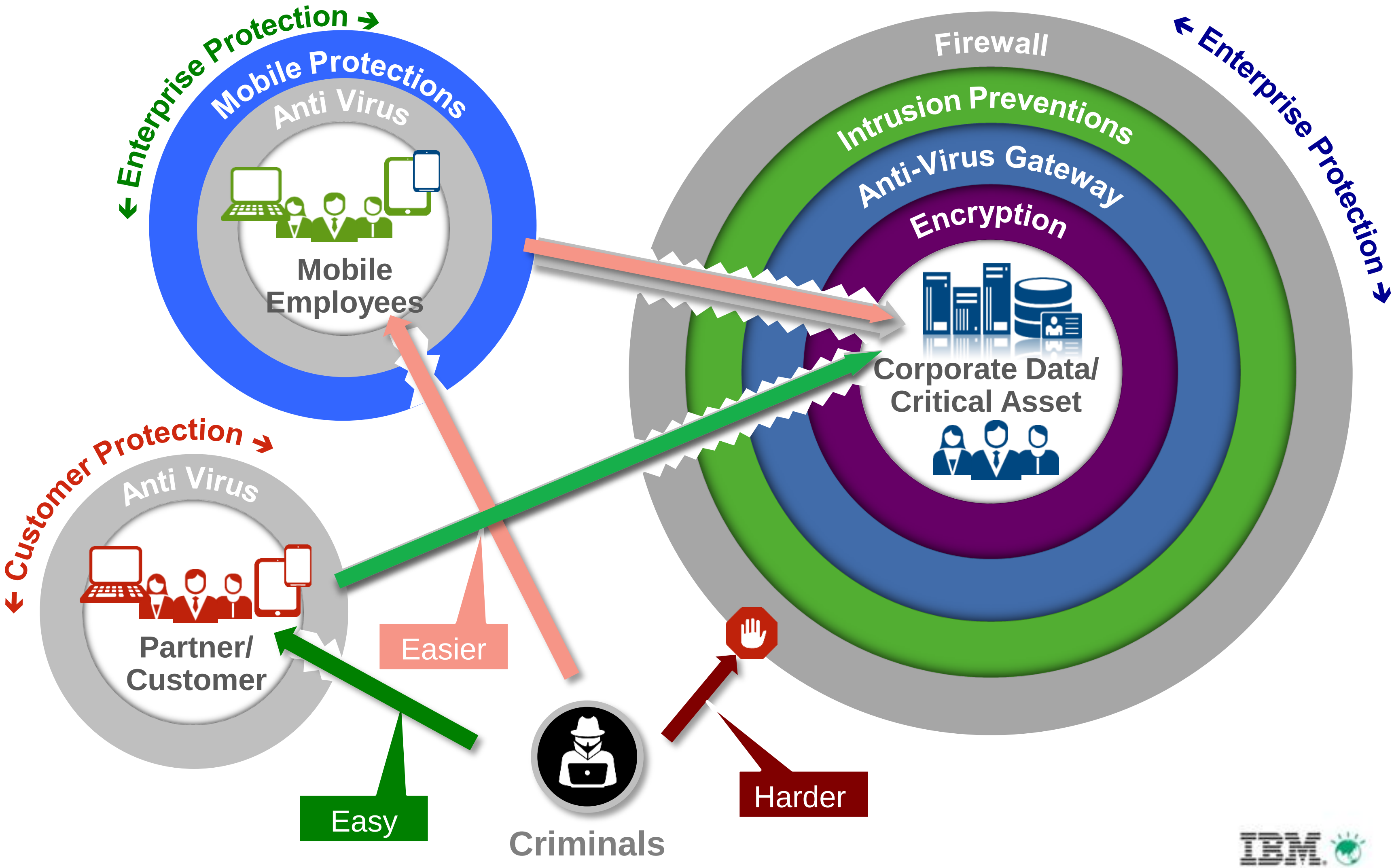
4444 3333 2222 1111

10 15 CVC-к

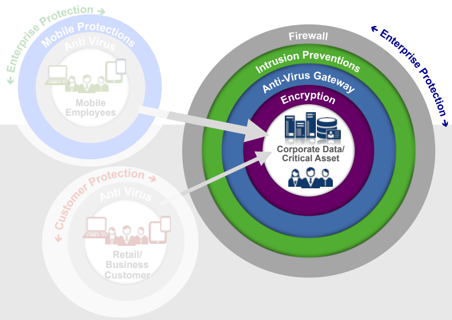
СОХРАНИТЬ

Criminals

進階持續性及針對式攻擊模式成為主流
人的疏失往往成為安全的最脆弱環節



新型態企業運作模式下的安全策略



1

保護好你的皇冠

Developing a crown Jewels Program

2

建立用戶保護模型

Persona Based Protection Model

3

從攻擊行為模式思考

Behavior Based Prevention

企業的關鍵資產保護攸關企業的永續經營
唯有有效辨識方能達到真正的保護

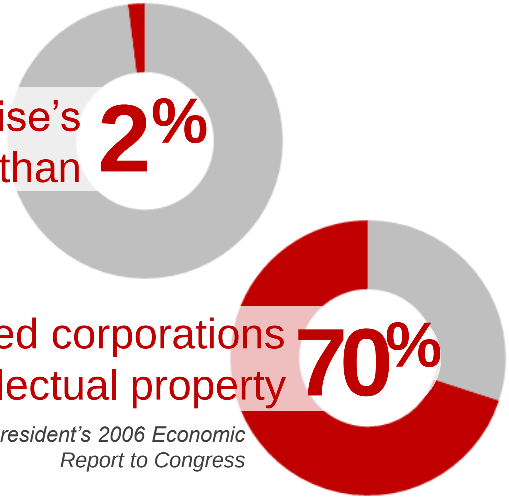
企業的關鍵資產的重要性不下於對皇冠上的珠寶的保護(Crown Jewels)

Crown Jewels
An organization's most sensitive or business critical information.

Today, many organizations are not aware of what their Crown Jewel information is, where it resides, who has access to it, or how it is protected.

Possessing information about Crown Jewels is necessary in order to determine whether adequate controls are in place.

Crown Jewel protection is dependent upon having access to vital information in order to apply proper controls.



Average enterprise's critical data is less than **2%**

Value of publicly traded corporations estimated to be intellectual property **70%**

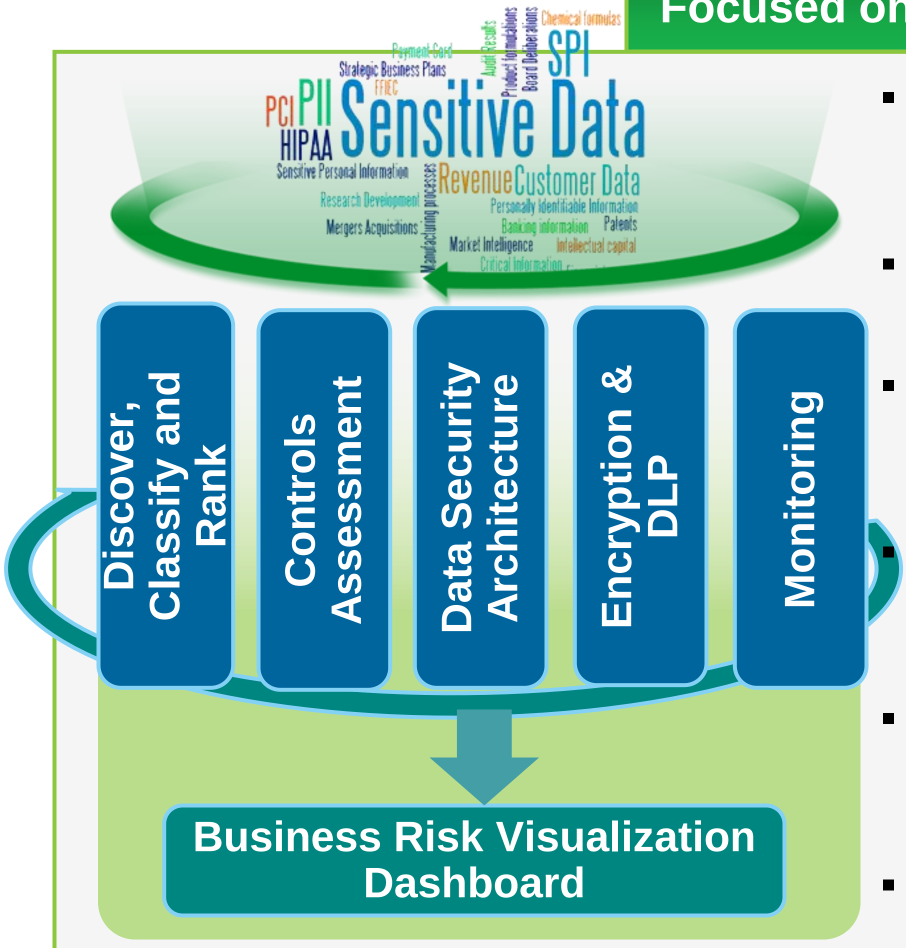
Source: U.S. President's 2006 Economic Report to Congress

Crown Jewel Examples

Enterprise	Executive
• Intellectual property • Top-secret plans and formulas	• Acquisition and divestiture plans • Executive and board deliberations

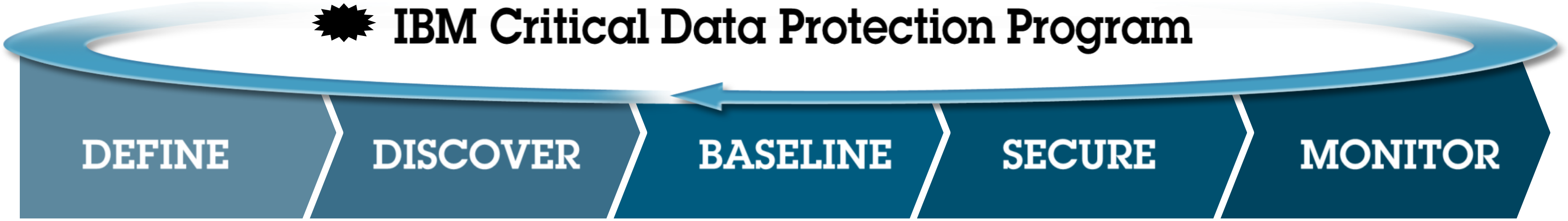
針對最關鍵的資產
評估及發展各種對應的資料防禦策略

Focused on protecting the most critical digital assets



- **Discover, Classify and Rank** identify the most critical digital assets – the organization "crown jewels" – in structured and unstructured repositories; repeat scans
- **Controls Assessment** identify and rank threats, review access privileges, and controls that are in place
- **Data Security Architecture** create a data security strategy and architecture for both structured and unstructured environments
- **Encryption & DLP** employ encryption and DLP technologies to protect the most valuable assets, the "crown jewels"
- **Monitoring** review monitoring metrics to ensure continued protection of "crown jewels" and adequacy of controls due to evolving threats
- **Business Risk Visualization Dashboard** to provide visual representation of risks to Critical Data assets and potential exposure of intellectual property (IP)

IBM 透過成熟的顧問方法論及工具導入
幫助客戶建立以關鍵資產為核心的保護模型



IBM Critical Data Protection Program

DEFINE

DISCOVER

BASELINE

SECURE

MONITOR

What are the “crown jewels”?

- *Determine data protection objectives*
- *Define “Crown Jewels”*
- *Develop organizational data model / taxonomy*
- *Obtain stakeholder consensus*

Where are they? How are they used?

- *Understand data lifecycle and environment*
- *Perform iterative discovery, analysis and classification*

What is required to protect critical data?

- *Establish baseline requirements*
- *Assess current data security processes and controls*
- *Determine gaps and identify solutions*

How to plan, design, and implement?

- *Plan and prioritize technical and business process transformations*
- *Design and implement solutions that protects critical data, enables access and aligns to business growth objectives*

What to consider operationally?

- *Determine metrics and process for monitoring, response, and communications*
- *Continue to evolve and adapt to changes*
- *Revalidate and improve program effectiveness*

Supported by:

Robust Consulting Method | Industry-specific Data Models | Global Consulting Expertise | IBM Data Security Research
IBM Guardium, StoredIQ, DLP and other leading data protection technologies

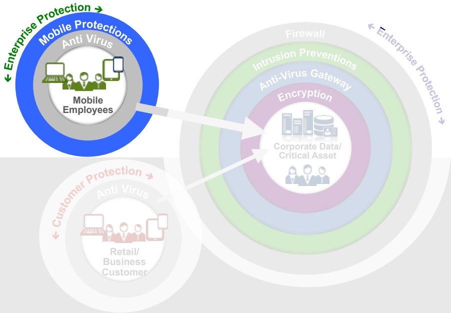
新型態企業運作模式下的安全策略

1

保護好你的皇冠
Developing a crown Jewels Program

2

建立用戶防護模型
Persona Based Protection Model



3

從攻擊行為模式思考
Behavior Based Prevention

企業逐步行動化的趨勢不易逆轉

They want their **Apps**

They need their **Content**

- Over 1M different apps managed
- 100,000+ apps in Enterprise App Stores
- Most active customers have 200+ different apps

Nearly 40% of customers push Secure Content to Devices and Users

- Intranet (40%)
- SharePoint (30%)
- File Shares (30%)

Mobile Content Management (MCM) is growing quickly!

行動化安全不僅要考慮設備本體，
網路通訊及應用端也都應該審慎考慮

At the Device

Manage device
Set appropriate security policies • Register • Compliance • Wipe • Lock

Secure Data
Data separation • Leakage • Encryption

Application Security
Offline authentication • Application level controls

Over the Network and Enterprise

Secure Access
Properly identify mobile users and devices • Allow or deny access • Connectivity

Monitor & Protect
Identify and stop mobile threats • Log network access, events, and anomalies

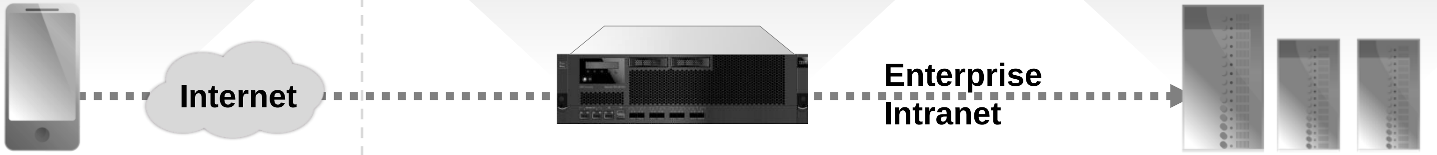
Secure Connectivity
Secure Connectivity from devices

For the Mobile App

Secure Application
Utilize secure coding practices • Identify application vulnerabilities • Update applications

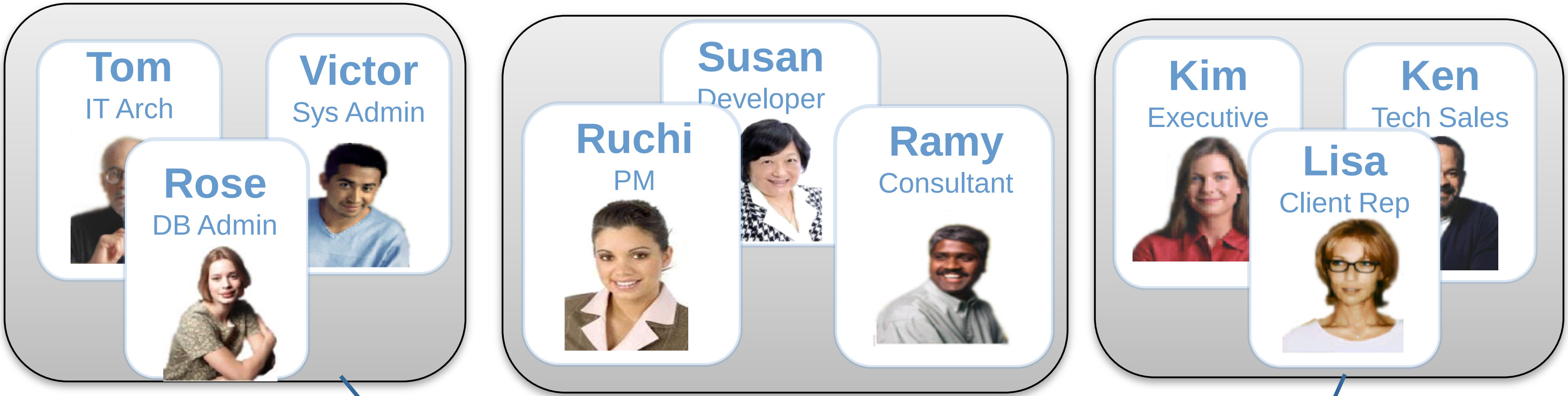
Integrate Securely
Secure connectivity to enterprise applications and services

Manage Applications
Manage applications and enterprise app store



IBM 本身從不同的員工的角色屬性
思考其對應行動化策略

User segments



Tom
IT Arch

Victor
Sys Admin

Rose
DB Admin

Susan
Developer

Ruchi
PM

Ramy
Consultant

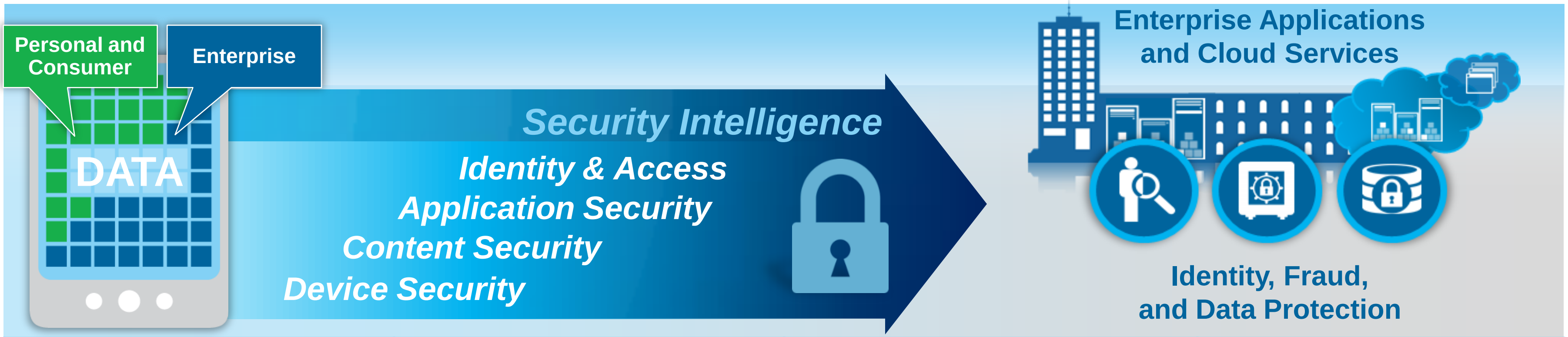
Kim
Executive

Ken
Tech Sales

Lisa
Client Rep

	Mobile Never	Mobile Optional	Mobile Enhanced	Mobile Primary
Capability segments	Voice only User never users mobile devices for IBM data	Core collaboration apps: Email/Calendar/Contacts, Connections, SameTime	Mobile Optional plus: File Sync / Backup, Core enterprise apps (w3 Intranet, Mgr tools, Expense & Time Reporting, etc.)	Mobile Enhanced plus: Productivity apps & print, role enablement apps (e.g., Sales = CRM, FMS, forecasting tool, etc)
Funding models		User funded (BYOD)	IBM or User funded	IBM funded

根據不同角色模型需求完整考慮
設備、傳輸、應用、存取管制等安全需求


Personal and Consumer

Enterprise

DATA

Security Intelligence

Identity & Access

Application Security

Content Security

Device Security

Enterprise Applications and Cloud Services

Identity, Fraud, and Data Protection

Device Security	*Content Security*	*Application Security*	*Identity & Access*
Provision, manage and secure Corporate and *BYOD* devices	Secure enterprise content sharing and segregate enterprise and personal data	Develop secure, vulnerability free, hardened and risk aware applications	Secure access and transactions for customers, partners and employees

IBM MobileFirst Protect (MaaS360)
Airwatch, MobileIron, Good, Citrix, Microsoft, Mocana

IBM Security AppScan, Arxan Application Protection, IBM Trusteer Mobile SDK
HP Fortify, Veracode, Proguard

IBM Security Access Manager for Mobile, IBM Trusteer Pinpoint
CA, Oracle, RSA

Security Intelligence

A unified architecture for integrating mobile security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management

IBM QRadar Security Intelligence Platform

新型態企業運作模式下的安全策略

1

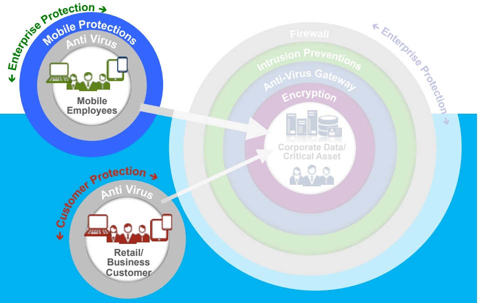
保護好你的皇冠

Developing a crown Jewels Program

2

建立用戶防護模型

Persona based Protection Model



3

從攻擊行為模式思考

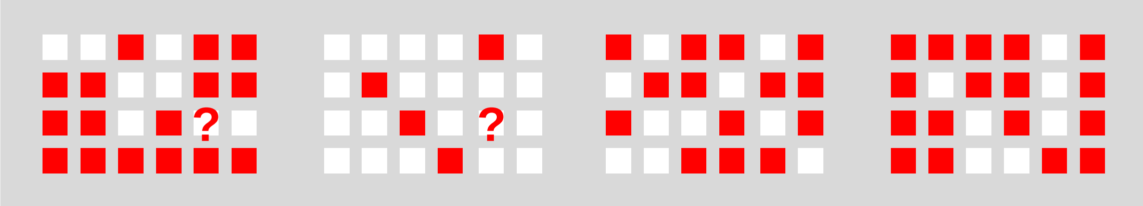
Behavior based prevention

傳統的威脅偵測模式易有盲點，
從攻擊者的行為模式著手可以建立新的防禦思維

LEGACY APPROACH

Anti-Virus
Focus: What it is

Files & Signatures (1000000s)

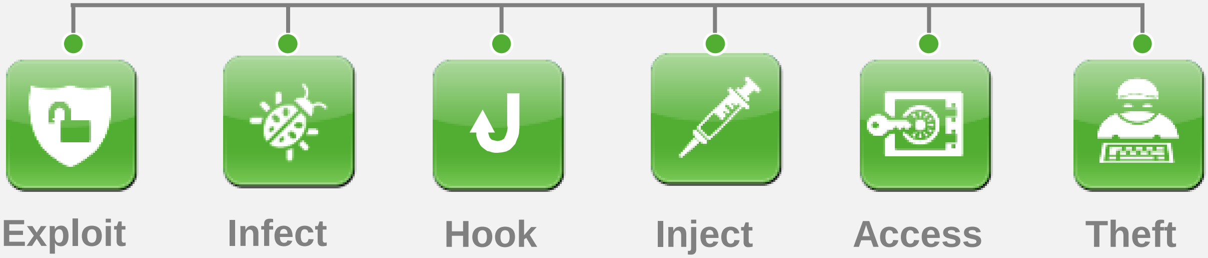


IBM Security Trusteer Rapport

IBM focuses on what matters
Focus: What it does

- Focuses on what the malware does

Crime Logic


Exploit

Infect

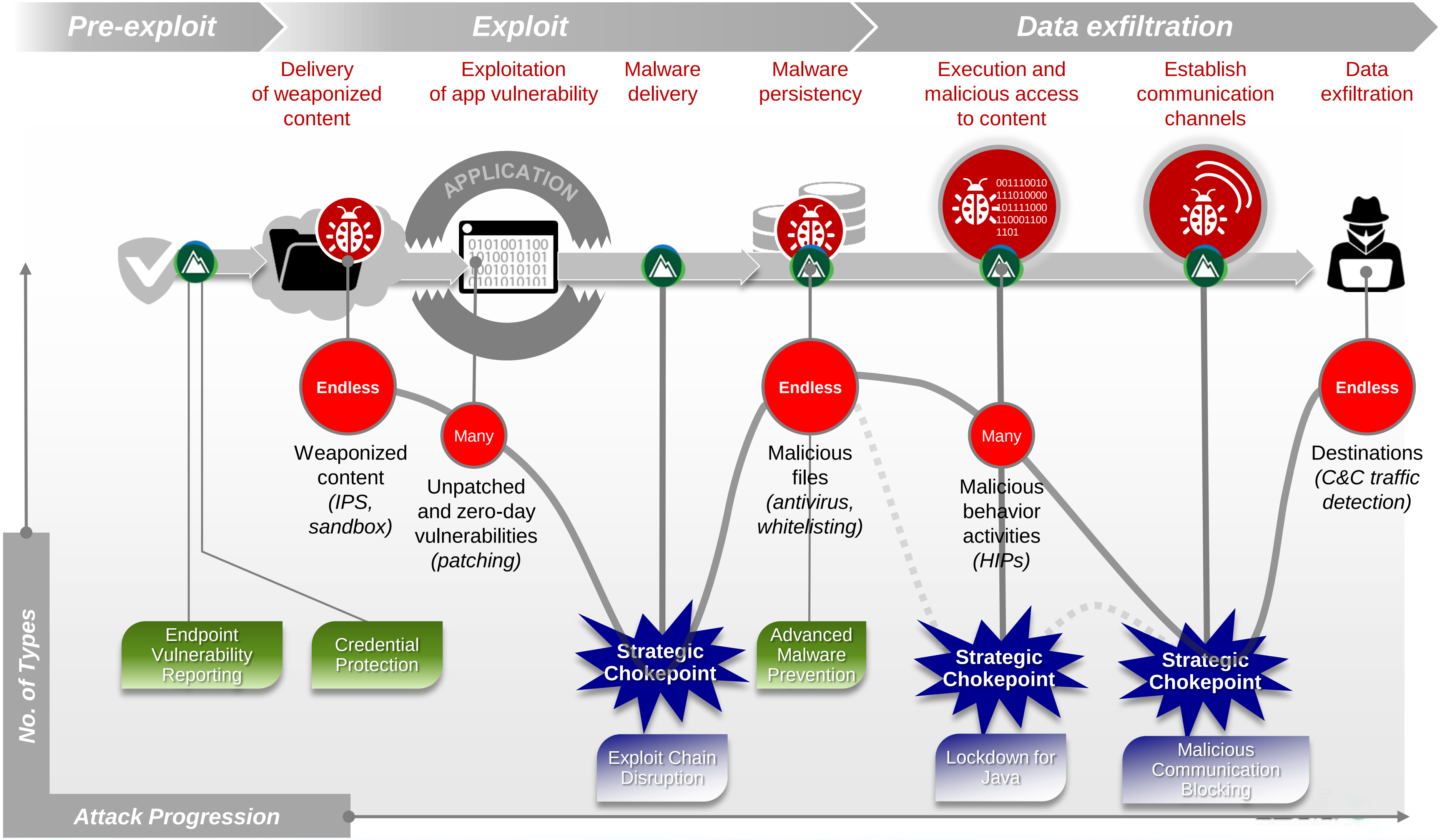
Hook

Inject

Access

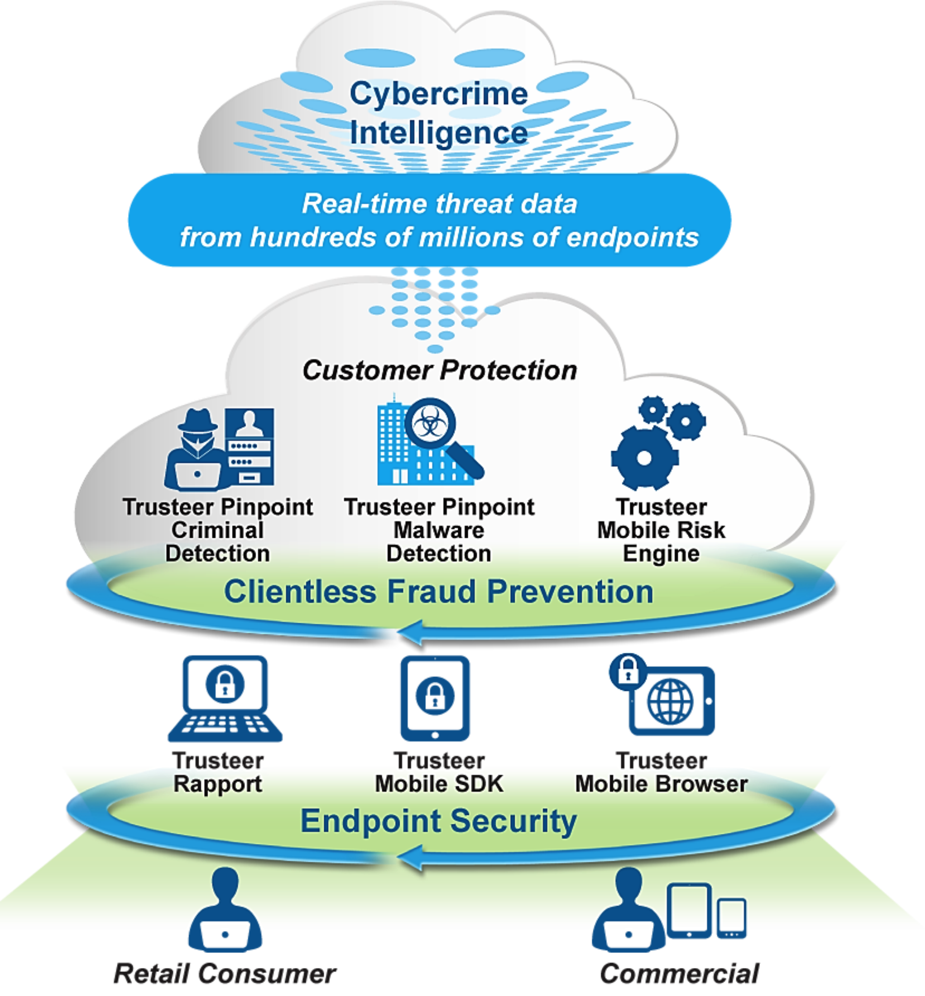
Theft

不同的威脅發展階段各有其特定的行為模式，在適當的關鍵防禦點阻擋可以收到事半功倍之效



透過攻擊行為模式防禦
避免客戶或合作夥伴成為安全斷鏈

Comprehensive platform for fraud detection and prevention


Cybercrime Intelligence
Real-time threat data from hundreds of millions of endpoints
Customer Protection
Trusteer Pinpoint Criminal Detection
Trusteer Pinpoint Malware Detection
Trusteer Mobile Risk Engine
Clientless Fraud Prevention
Trusteer Rapport
Trusteer Mobile SDK
Trusteer Mobile Browser
Endpoint Security
Retail Consumer
Commercial

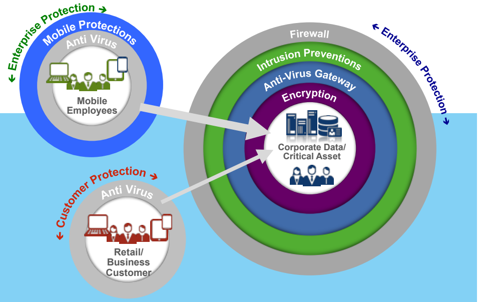
Clientless Fraud Prevention

- **Trusteer Pinpoint Criminal Detection**
  Evidence-based detection of account takeover attempts
- **Trusteer Pinpoint Malware Detection**
  Real-time malware detection
- **Trusteer Mobile Risk Engine**
  Detects mobile-fraud risks from compromised end user and criminal-owned devices

Endpoint Security

- **Trusteer Rapport**
  Prevents and removes financial malware and detects phishing attacks
- **Trusteer Mobile SDK**
  Embedded security library for native apps that detects compromised / vulnerable devices
- **Trusteer Mobile Browser**
  Risk-based analysis of mobile web access

新型態企業運作模式下的安全策略



1

保護好你的皇冠

Developing a crown Jewels Program

2

建立用戶保護模型

Persona Based Protection Model

3

從攻擊行為模式思考

Behavior Based Prevention

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