

Hong Kong Computer Society

Information Security Specialist Group

Cecil Siu
Programme Committee
Member, HKCS-ISSG
(cecil.siu@utimaco-asia.com)



hkcs.org.hk

About HKCS

- Founded in 1970 as a Professional Institution for the field of information technology
- providing service and support to the IT community, including individual practitioners, employers of IT staff and the general public.

*Serving Hong Kong IT Industry and
Community for over 30 years*



HKCS Mission

To accelerate the understanding, adoption, use and widespread acceptance of Information Technology (IT) through educational programs, advocacy, industry relations and by bringing together, in an open forum, leading users and technologists from both the public and private sectors

Specialist Groups

- *Information Security Specialist Group (ISSG)*
- *Database Specialist Group (DBSG)*
- *e-Business Specialist Group (eBizSG)*
- *Software Quality and Software Process (HKSPIN)*
- *Internet & Networking Specialist Group (INSG)*
- *Linux Specialist Group (LinuxSG)*
- *Multimedia Specialist Group (MMSG)*
- *eXtensible Markup Language Specialist Group (XMLSG)*



New Trends of Mobile Data Protection



hkcs.org.hk



Today's Challenges



hkcs.org.hk

Today's Challenges

- Over 20 high profile breaches in the last 12-18 months.

- Since 2005: More than **97 million records** containing sensitive personal information were involved in security breaches.

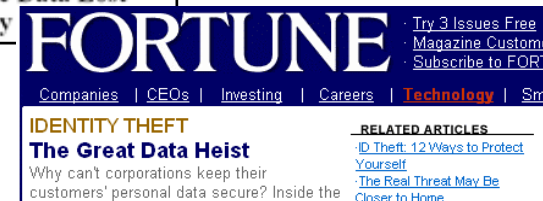
(Source: www.privacyrights.org/ar/ChronDataBreaches.htm, 11/2006)

- Every **53 seconds** a laptop is stolen

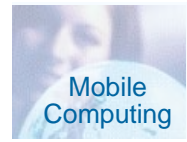
(Source: http://www.usatoday.com/tech/news/computersecurity/2006-11-19-lockdown-laptop_x.htm)

- 90% of companies** detected security breaches in last 12 months

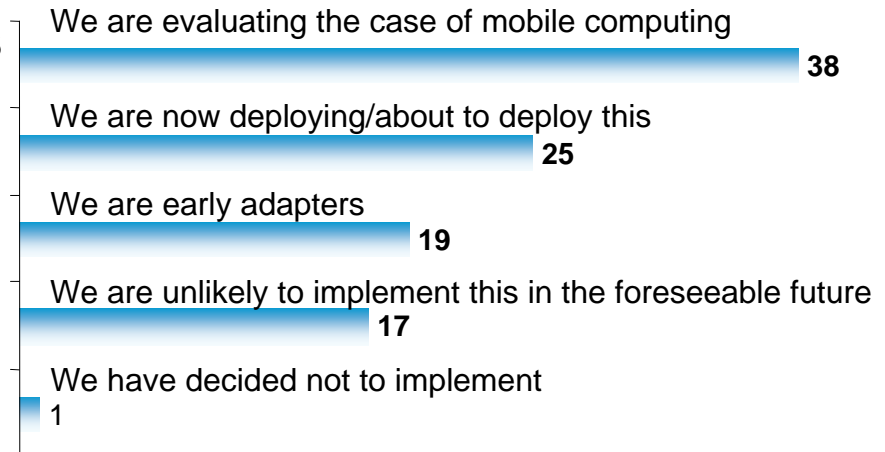
(Source: Federal Bureau of Investigation, 2006)



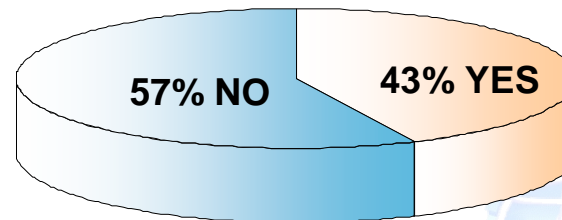
Company's Attitude to Mobile Computing



- Which of the following options best describe your company's attitude to mobile computing? (% of respondents)

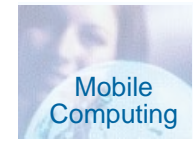


- We have set budget aside for investments in mobile computing technology



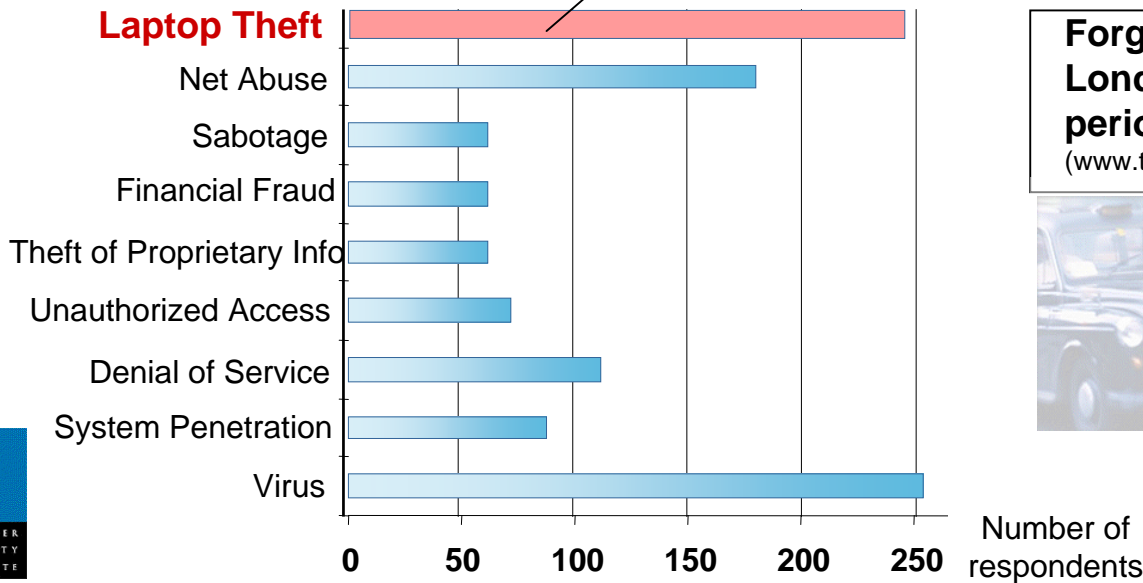
Work goes Mobile

Enhanced Security Risks



- 10% of all notebooks gets stolen or gets lost (annually)
(Web & Collaboration Strategies 2003)

Types of attacks and misuse



CSI/FBI: Computer Crime and Security Survey 2003

Forgotten notebooks in London Taxis during a 6 months period: → 5000 pieces
(www.theregister.co.uk/2005/01/25/taxi_survey)



“disappeared”

- 60 % of all corporate data assets reside unprotected on PCs, Notebooks and Removable Media (Search Security Newsletter, April, 2003)
- Hard disk is the weakest point (Informationweek Nr. 24/2003)
- FBI estimates: 57% of unauthorized intrusions into corporate servers are made possible through stolen notebooks



Work goes Mobile

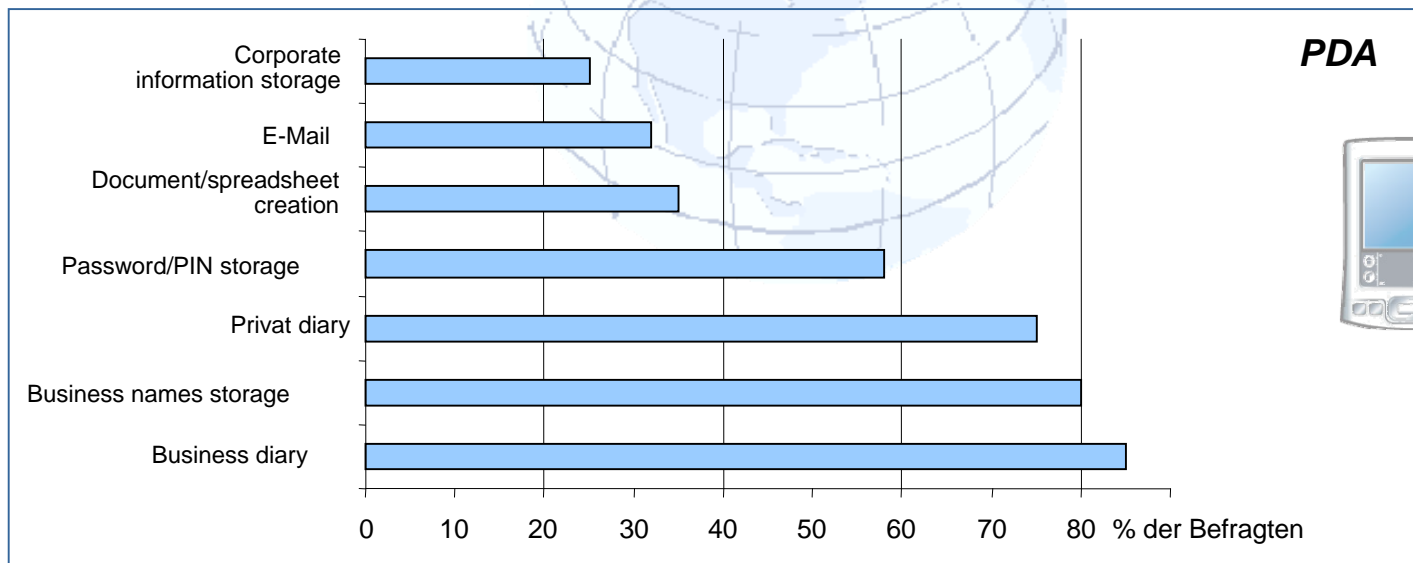
Special Risks with Handheld Devices



User Habit:

- 57% neglect to encrypt corporate data on their PDAs.
- 41% utilize their PDAs to access corporate networks
- 25% bypassing the password function.

PDA used for various activities:



PDA Usage Survey for 2004, *ComputerWeekly* and Reed Exhibitions
http://www.usatoday.com/tech/columnist/ericjsinrod/2003-08-21-sinrod_x.htm



Compliance & IT Security



hkcs.org.hk

SOX

Sarbanes Oxley Act

Why SOX?

Whether it's Enron, Parmalat or someone else, the symptoms are falsified balance sheets, failing to announce profit warnings, insider trading, and a lack of controls and transparency.

Quick facts

- Law for monitoring the financial data of companies listed on the stock exchange, defining requirements for in-house IT
- Compulsory for US companies listed on the Stock Exchange (since 2004)
- Companies listed on US stock exchanges are subject to SOX, no matter where they have their headquarters (from May 2005)
 - Focus on management responsibility for setting and implementing the appropriate internal controls and processes for financial reporting.
 - Implementation of IT risk management plays a central role.
 - The CEO and CFO are personally liable for the implementation of control mechanisms. They will be fined up to \$5 million or jailed for up to 20 years if they intentionally deceive shareholders.

IT security is a legal duty of executive management



SOX

Sarbanes Oxley Act



Quick facts

- Implementation of IT risk management plays a central role.
- In any case, the following applies:
 - If a company conforms with the SOX regulations, banks and capital markets will regard it as highly trustworthy.

IT security is a legal duty of executive management

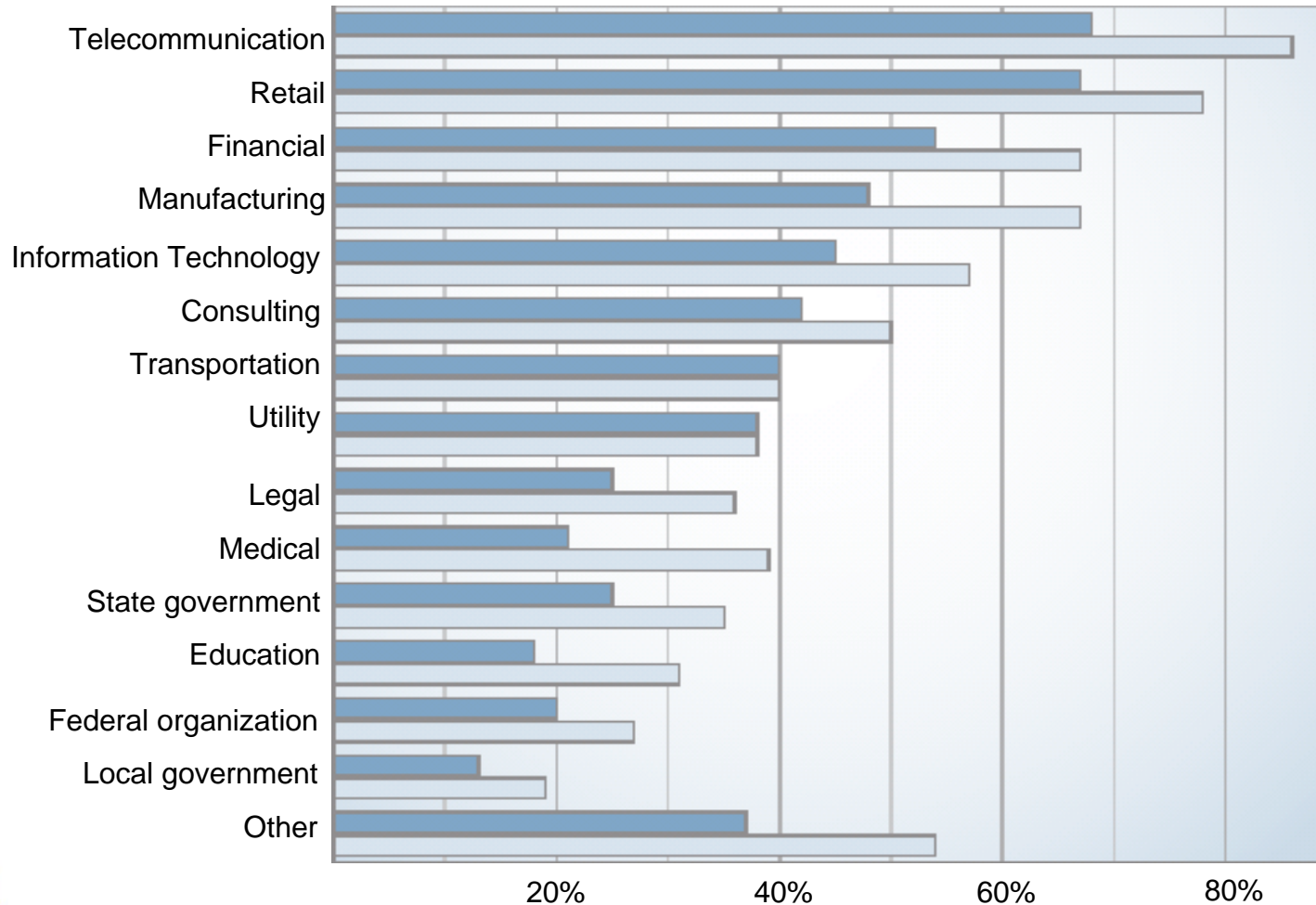


SOX

Sarbanes Oxley Act

- Changed focus from technology to corporate governance
- Raised level of interest in information security

Impact on Information Security



Source: CSI / FBI Computer Crime and Security Survey 2006, 601 Respondents



EU Directive 95/26/EG



Quick facts

- EU Directive 95/26/EG outlines how the personal data of citizens is to be protected
- It also defines a citizen's rights over their data
- EU Member States had to add this directive to their own legislation by 1998.

IT security is a legal duty of executive management

Compliance

Primary Focus (Extract)



Regulation	Country	Topic
HIPAA Health Insurance Portability and Accountability Act	USA	Protection of patients data
GLBA Gramm-Leach-Bliley Act	USA	Protection of personal financial data
SB 1386 California Senate Bill 1386	CA, USA	Protection of personal data of residents in the state of California
PIPEDA Personal Information Protection and Electronic Documents Act	Canada	Protection of personal data in business relations
PIPL Personal Information Protection Law	Japan	Protection of personal data
DPA Data Protection Act	UK	Protection of personal data
95/46/EC European Union Directive	Europe	European data protection directive
SOX Sarbanes-Oxley Act	USA (worldwide)	Increased liability of companies concerning the presentation of business development
Basel II	Europe	Policies to control and mitigate operational risk. Optimization of risk management as necessary

Compliance

Primary Focus (Extract)



Regulation	Country	Topic	
HIPAA Health Insurance Portability and Accountability Act	USA	Protection of patients data	
GLBA Gramm-Leach-Bliley Act	USA	Protection of personal financial data	
SB 1386 California Senate Bill 1386	CA, USA	Protection of personal data of residents in the state of California	
PIPEDA Personal Information Protection and Electronic Documents Act	Canada	Protection of personal data in business relations	
PIPL Personal Information Protection Law	Japan	Protection of personal data	
DPA Data Protection Act	UK	Protection of personal data	
95/46/EC European Union Directive	Europe	European data protection directive	
SOX Sarbanes-Oxley Act	USA (worldwide)	Increased liability of companies concerning the presentation of business development	
Basel II	Europe	Policies to control and mitigate operational risk. Optimization of risk management as necessary	



= Primary focus: Data confidentiality (based on encryption)



IT Security Impact of Compliance

Regulation Technology	US SOX	Europe Basel II	Germany KonTraG	US HIPPA	CA SB	US GLBA	Canada PIPEDA	Japan PIPL	UK DPA	Europe 95/46/EC	Germany BDSG
Business Intelligence	X	X	X								
Document Management	X	X	X	X	X	X					
Records Management	X	X	X	X	X						
Archiving	X	X	X	X	X	X					
Security	X	X	X	X	X	X	X	X	X	X	X
Storage	X	X	X	X	X						

Extract of governmental regulations

- 74% of all enterprises expect to spend more time and money in 2007 on information security due to **compliance and privacy regulations**

Deloitte: Security Survey 2006 - Protecting the digital assets

Topic: Confidential data at risk



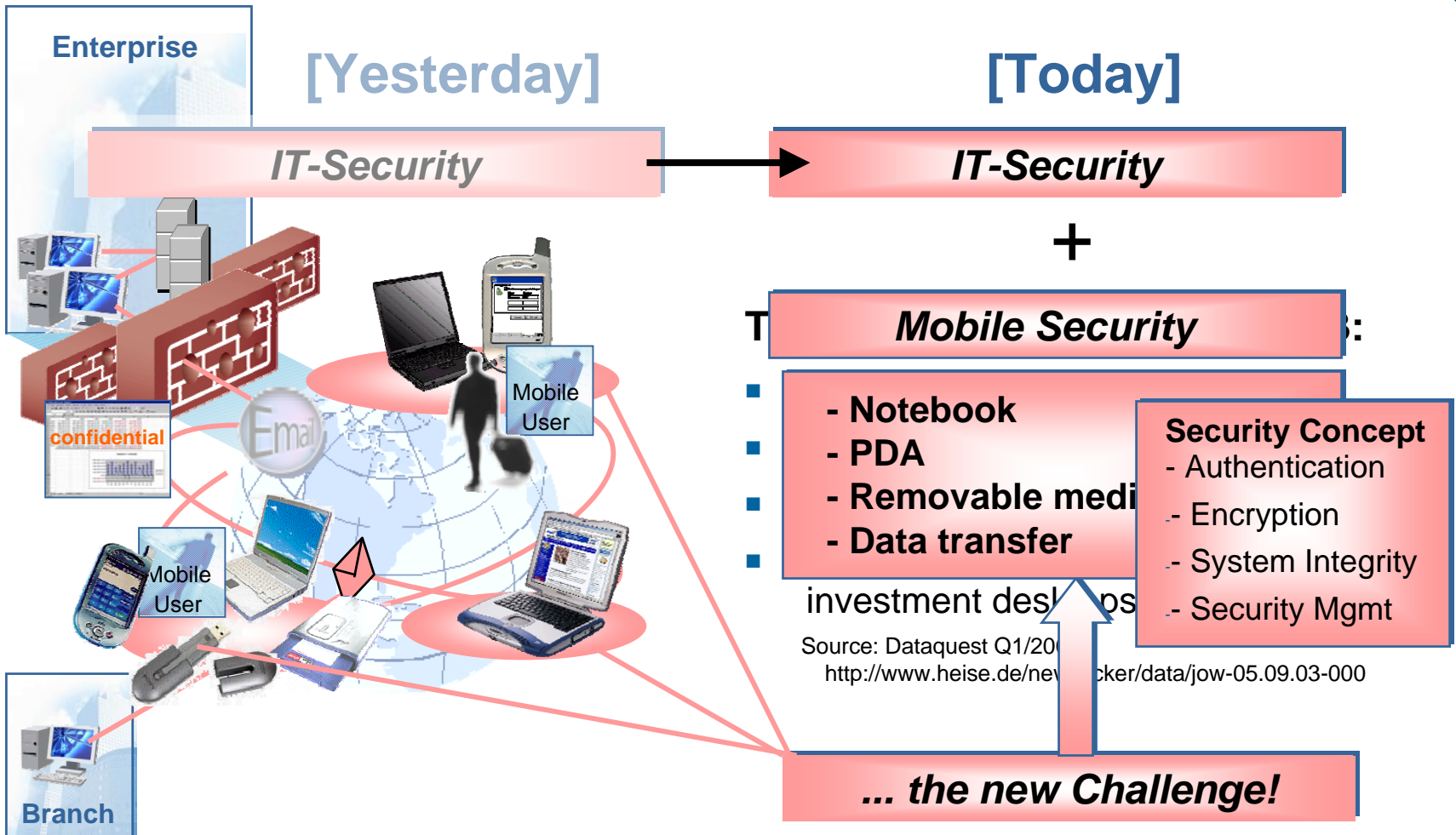
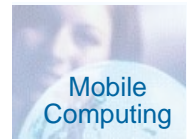
IT Security

Compliance: Rules? What Rules?

- The consequences of non-compliance are very serious:
 - Prison sentences for senior executives & board members (up to 20 years)
 - Incredibly high fines (up to \$5 million)
 - Possible loss of insurance cover
 - Risk of losing creditworthiness
 - Auditors refuse to grant attestation
 - Loss of image and reputation
 - Further financial penalties
 - Increased risks of liability

IT Security: Not just about investment
but a prerequisite for covering business risks

IT-Security





[Data Security Requirement]

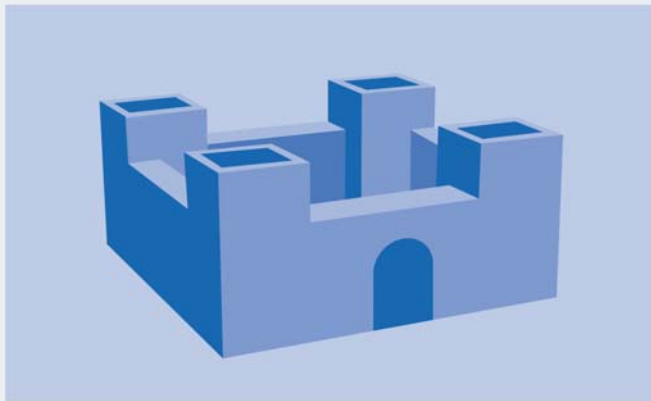


hkcs.org.hk

Data Security Requirements

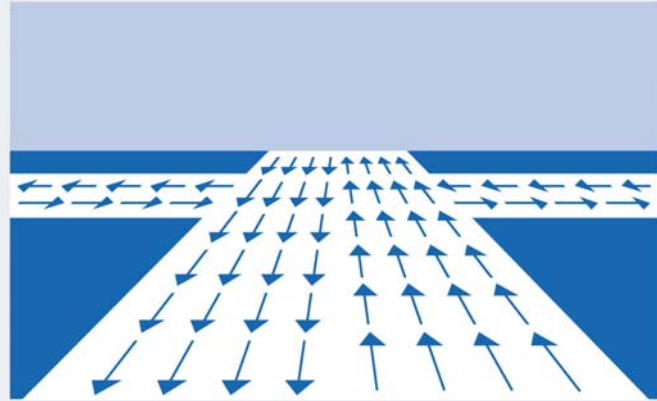
1. Safeguard Your Data – not just the Infrastructure

Walling Off Security



- Firewalls and Security Gateways protect the company perimeter
- Let the “good guys” in, keep the “bad guys” out
- Closed shop with own policies, and rules

Open Enterprise Security

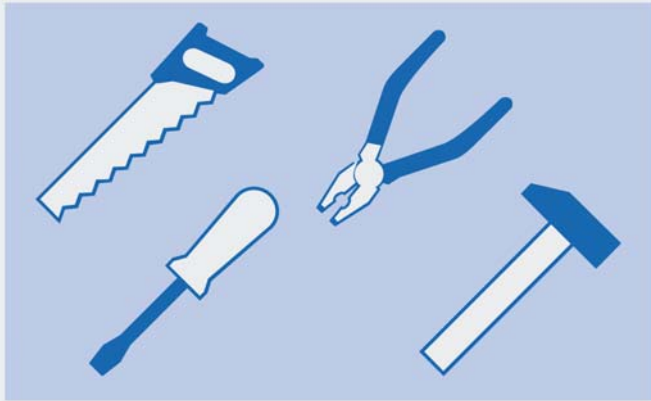


- Cross-company processes
- Open IT Infrastructures
- Bad guys and good guys may be in already
- Data-level protection
- Safeguard the end point and the individual transaction

Data Security 2.0 Requirements

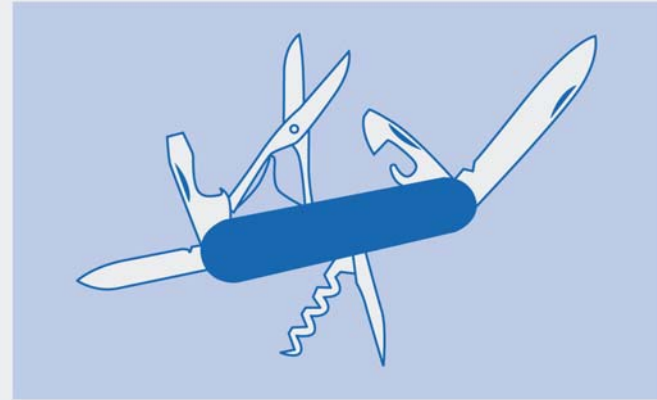
2. Shift from a “Tool Mindset” to an Integrated Approach

Fragmented Solutions



- Proprietary point security solutions
- No central policy management & enforcement
- Difficult for users and administrators
- Costly and often not scalable

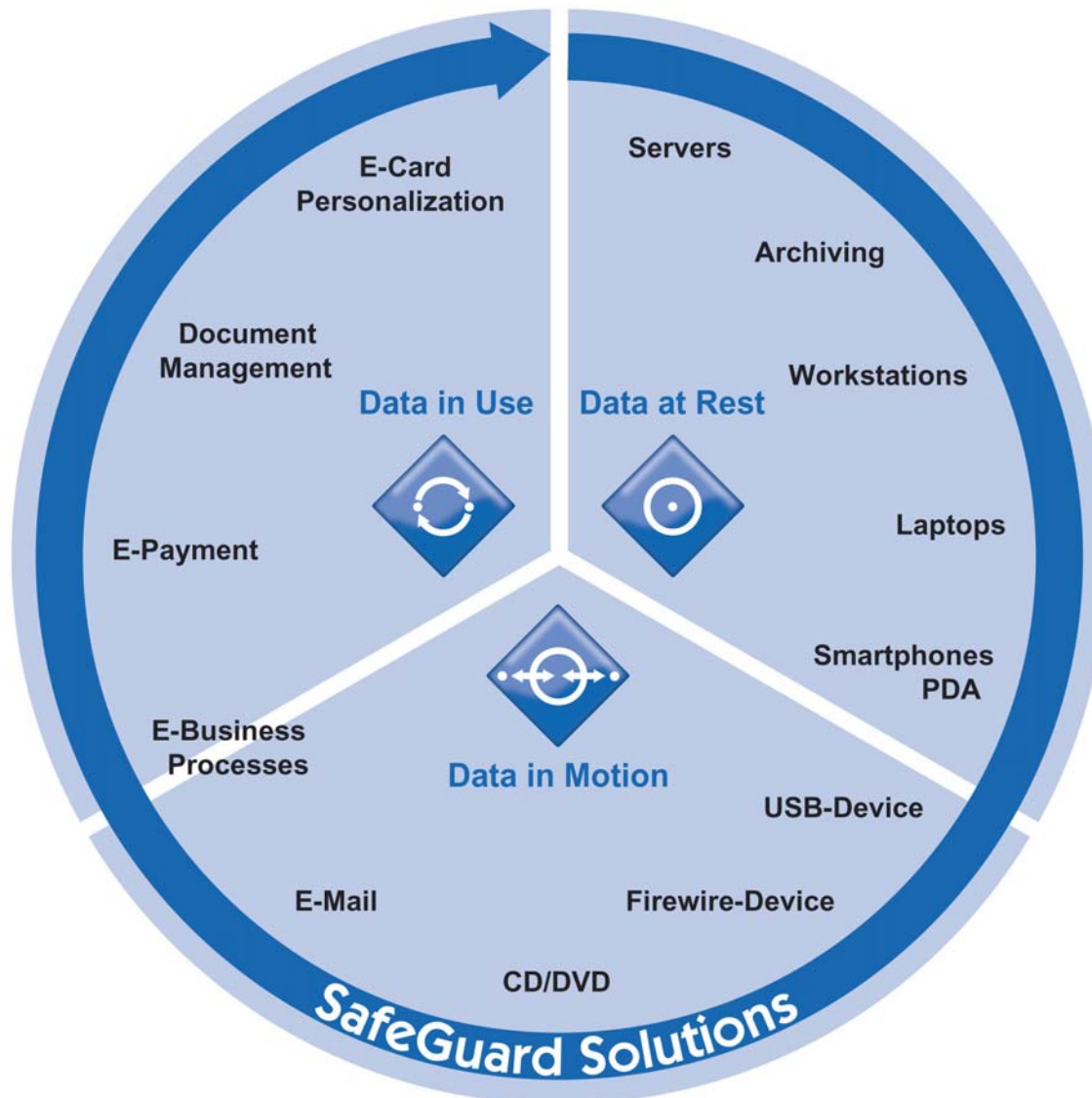
Integrated Solutions



- Integration instead of pure best-of-breed
- Transparency and manageability
- Reduces costs by decreasing the burden for end-users and administrators

Data Security 2.0 Requirements

3. Embrace a 360° Approach to Data Security





End-point Devices Protection



hkcs.org.hk

[End-Point Device Protection]

→ *Functionality at a glance*

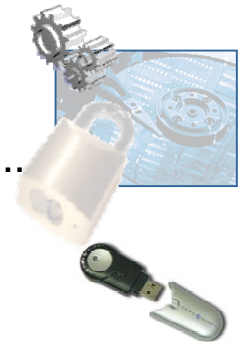
[SafeGuard] for Mobile Security

Entire hard disk encryption as protection of data in case of PC or Notebook theft/loss

- Power On Authentication (PoA)
 - User ID+ password before OS starts
 - Can not be circumvented
 - eToken Support optional
- Data encryption (sector level)
 - User transparent, on the fly
 - Entire hard disk incl. OS, Hibernation, Tempfiles,...
 - Removable Media
 - Strong algorithms (IDEA, AES, ...)
 - Hibernation support
- Emergency-Tools
 - Challenge-Response functions to reset lost PW
 - Repair Functions, MBR protection (automatically)
 - Support Rescue and Recovery (Lenovo -TVT)



Electronic Fortress



[End-Point Device Protection]

→ *Functionality at a glance*

[SafeGuard] for Mobile Security

- Easy for the User
 - User friendly + transparent
 - No changes to work behaviour
 - Reduces the users responsibility for security
- Easy for the Administrator
 - Unattended installation via config.files via network
 - No additional support costs (fully transparent for user)
 - “Emergency tools” (e.g. new password via phone)
- Safe solution with strong encryption algorithms
 - Protection of all data against outsiders (power off mode)
 - Secure login with user ID and PW
 - Encryption on sector level on hard disk & external devices
 - “Fixed” Security Policy
 - Certified trustworthy software
 - Secure Hibernation

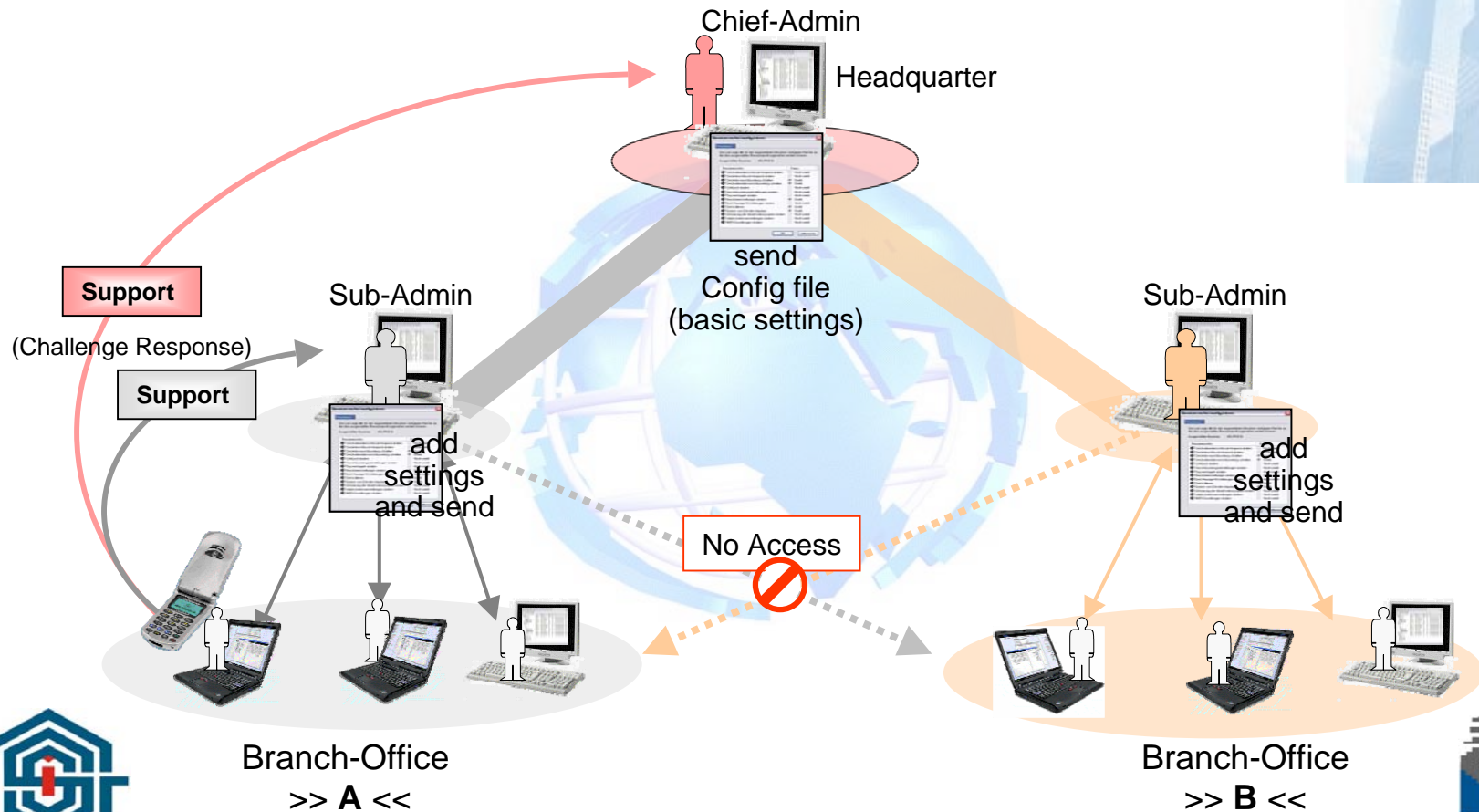
[End-Point Device Protection]

→ Security Hierarchy

Admin

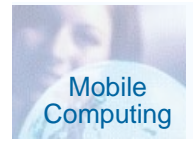
■ Extended Administration Concept

- Definition of "Sub-Administrators", with limited rights in a pre-defined configuration file

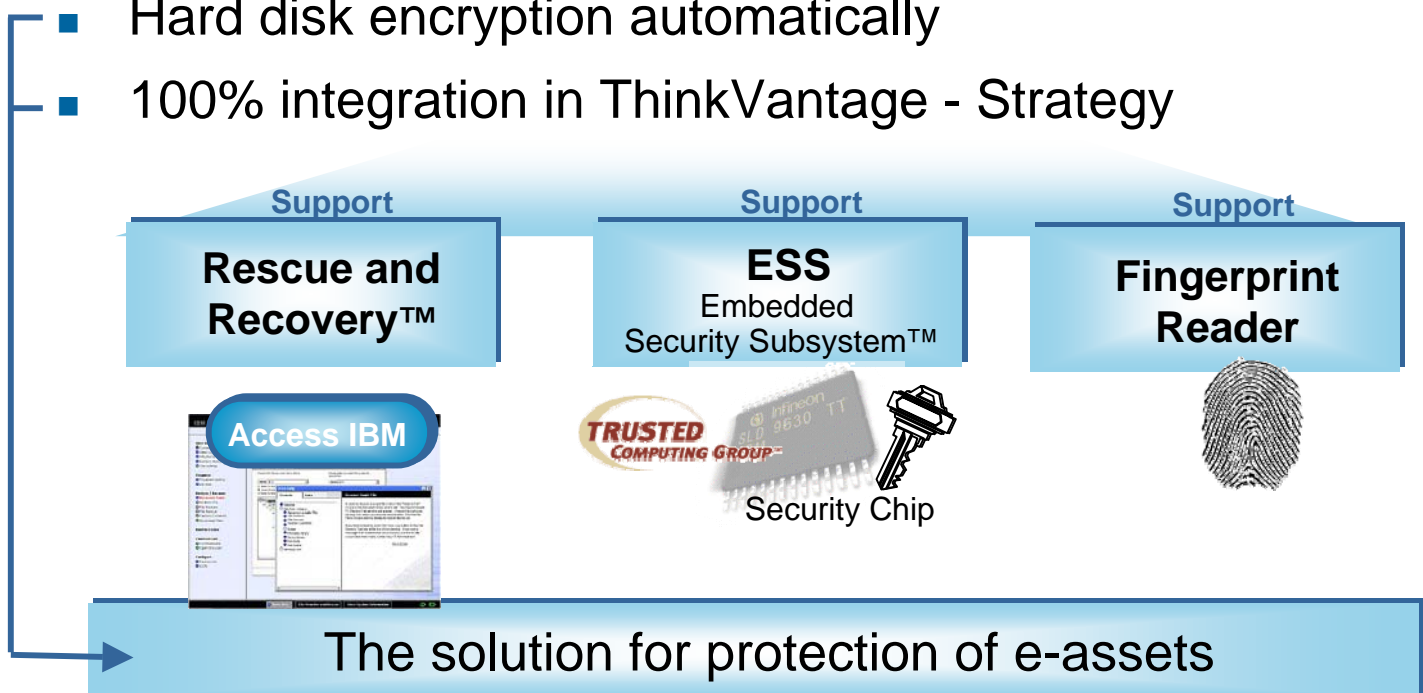


[End-Point Device Protection]

→ Biometric Authentication



- Unique security solution for access control and data confidentiality on all ThinkCentres™ and ThinkPads®.
- Hard disk encryption automatically
- 100% integration in ThinkVantage - Strategy



100% compatible with ThinkVantage™ Technology

Security Made Easy



[PDA Device Protection]



hkcs.org.hk

[PDA Device Protection]

→ *Functionality at a glance*

- Biometric Signature Logon
 - Authentication by a handwritten „password“
 - Checks form and dynamics (speed)
 - Fast and convenient
- Symbolic Logon
 - Create a "story" from symbol sequence to remember PIN easily
 - Very fast authentication, configurable layout
- Password Logon
 - More flexible password rules than in OS
 - Allows to create complex passwords
- Fingerprint Logon
 - E.g. IPAQ 545x / 555x
 - Optional password login fallback
- *For ActiveSync protection on PC, always the user password is used*



[PDA Device Protection]

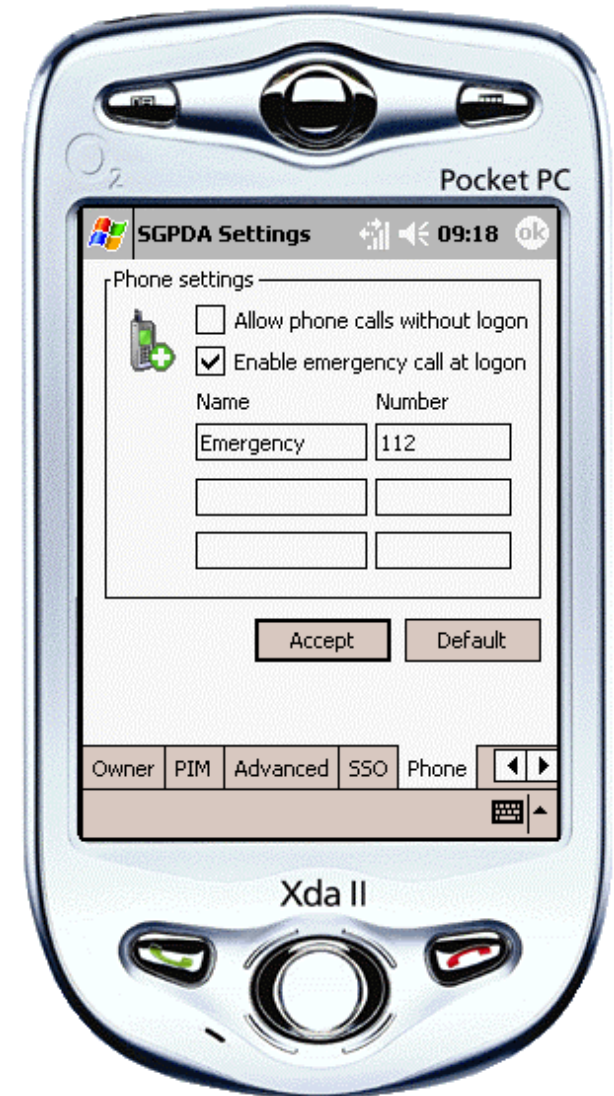
→ *Functionality at a glance*

- **PIM Encryption**
Separately configurable encryption of calendar, contacts, to-do lists, e-mails and e-mail attachments
- **Configurable "Notification" behavior**
Allows selection whether calendar alarm notifications or SMS shall be visible for the user without authentication
- **Secure Screensaver**
PDA may be automatically locked now after a given time of user inactivity without requiring to turn the PDA off
- **Bluetooth / WLAN / Phone blocking**
in addition to infrared, now also these functions may be centrally disabled
- **Unrestricted Phone Function**
Allows optionally using the phone application without authentication (convenience, also for Personal Edition available)
- **Policy Import in Administration (in addition to Export)**
Allows the efficient migration of settings e.g. from test to productive environment
- **Event Logging**
Logging of relevant events e.g. "false logon try" on PDA

[PDA Device Protection]

→ *Additional Functionality at PDA Phone/SmartPhone*

- User can receive calls and SMS without authentication at
- Option: User can make calls without authentication
- Configurable "emergency numbers" that can be called without authentication
- Optional GSM SIM lock prevents that SIM card is changed without central approval
- Network connection may remain active when device display is locked (e.g. for file download)
- Option: Phone functionality can be blocked (entering a SIM card blocks the phone)

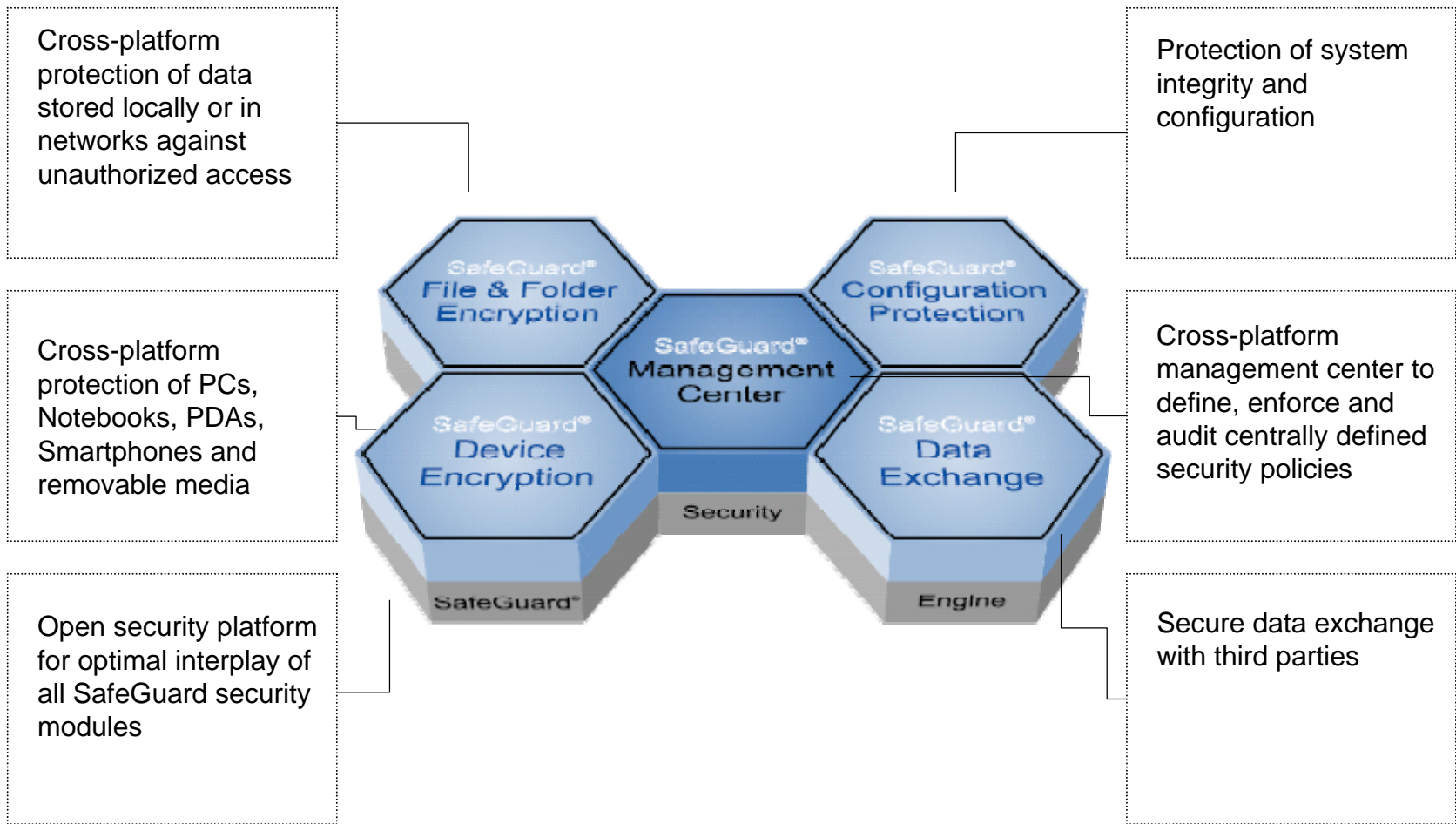


[Integrated Data Security]



hkcs.org.hk

Next Trends of Mobile Data Security Suite



Cross-platform data security for all desktops and mobile devices

Membership Grades

- **Professional Class**
 - **Fellow Member (FHKCS)**
 - **Full Member (MHKCS)**
 - **Associate Member (AHKCS)**
- **Technician Class**
 - **Practitioner Member**
- **General Class**
 - **Graduate Member**
 - **Student Member**
 - **Affiliate Member**
 - **Corporate Member**
 - **Honorary Member**



Special Offer

ACT now!! Sign up today to receive special offer:

Individual Membership - HK\$300 waiver on entrance fee or

Corporate Membership - 20% discount on first year annual fee!!





HONG KONG
COMPUTER
SOCIETY

**Contact for Membership:
Hong Kong Computer Society**

Telephone: 852-2834 2228

Fax: 852-2834 3003

www.hkcs.org.hk

Email: Membership@hkcs.org.hk

Interested on Today Presentation

Cecil Siu

cecil.siu@utiamco-asia.com