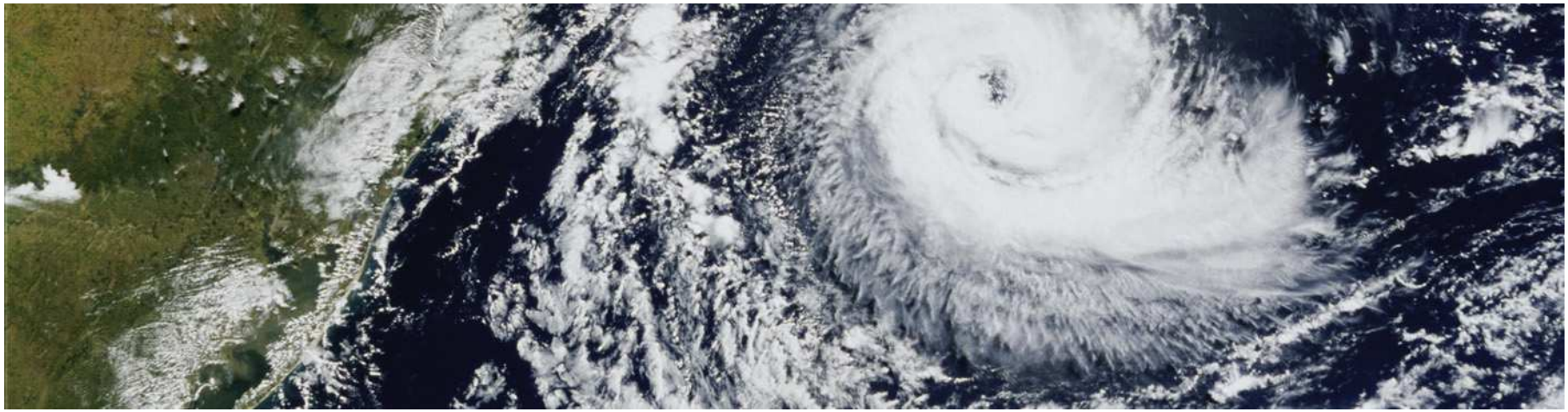
IT security



Is Security really a need ?

**"Information security is a major priority at this company.
We've done a lot of stupid things we'd like to keep secret."**

Security pains impact business

Security Pain	***Business Impact***
▪ Difficult to *protect sensitive information* about employees, customers, partners	▪ Impaired employee and partner relations; lost customers; compromised reputation; regulatory and legal exposures
▪ Users can't keep up with *multiple passwords*; call help desk for resets	▪ Low user productivity and satisfaction; high support costs
▪ *Security breaches* affect Web sites, users, networks… -Hackers, disgruntled employees, denials of service, worms/viruses…	▪ Business processes disrupted - Lost sales, idle employees, damaged reputation
▪ Multiple *inconsistent*, *often manual* security processes -Each new application requires a new security and access process.	▪ Lack of business flexibility and speed; slow response to market requirements - Higher length, cost and complexity of the application development cycle

IT security strategy, plans and capabilities may not match rising business expectations.

Security perception has changed

security =110

☞ Cyber Attacks generate 110 $ Billons revenue

☞ 110 millions customer data stolen to a single company in less than one week

So …

Cost is not really a KPI for Security …

The impact and visibility of recent breaches calls into question the effectiveness of traditional security measures

SONY (2011)
Brand impact, remedies & lost business = $1B loss est.

Hackers exploited Web application vulnerability to access back-end customer databases

CYBER-ACTIVISM

STUXNET(2010)
Targeted changes to process controllers refining uranium

IMPACT
Degraded ability to safely process and control highly volatile materials

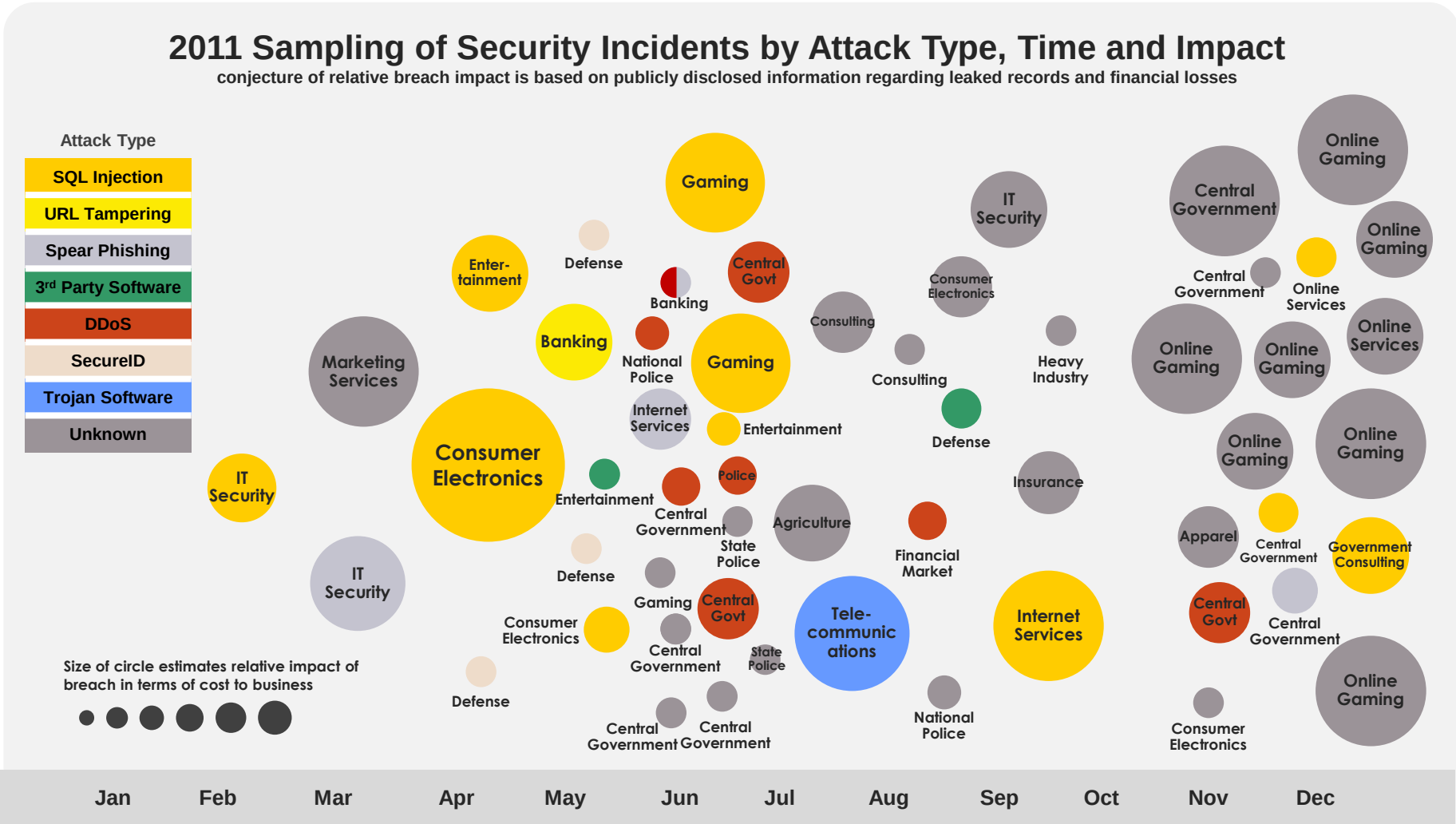
CYBER-WAR

Target(2013)
Theft of 130 millions customer data sent to ???

IMPACT
TBD ….

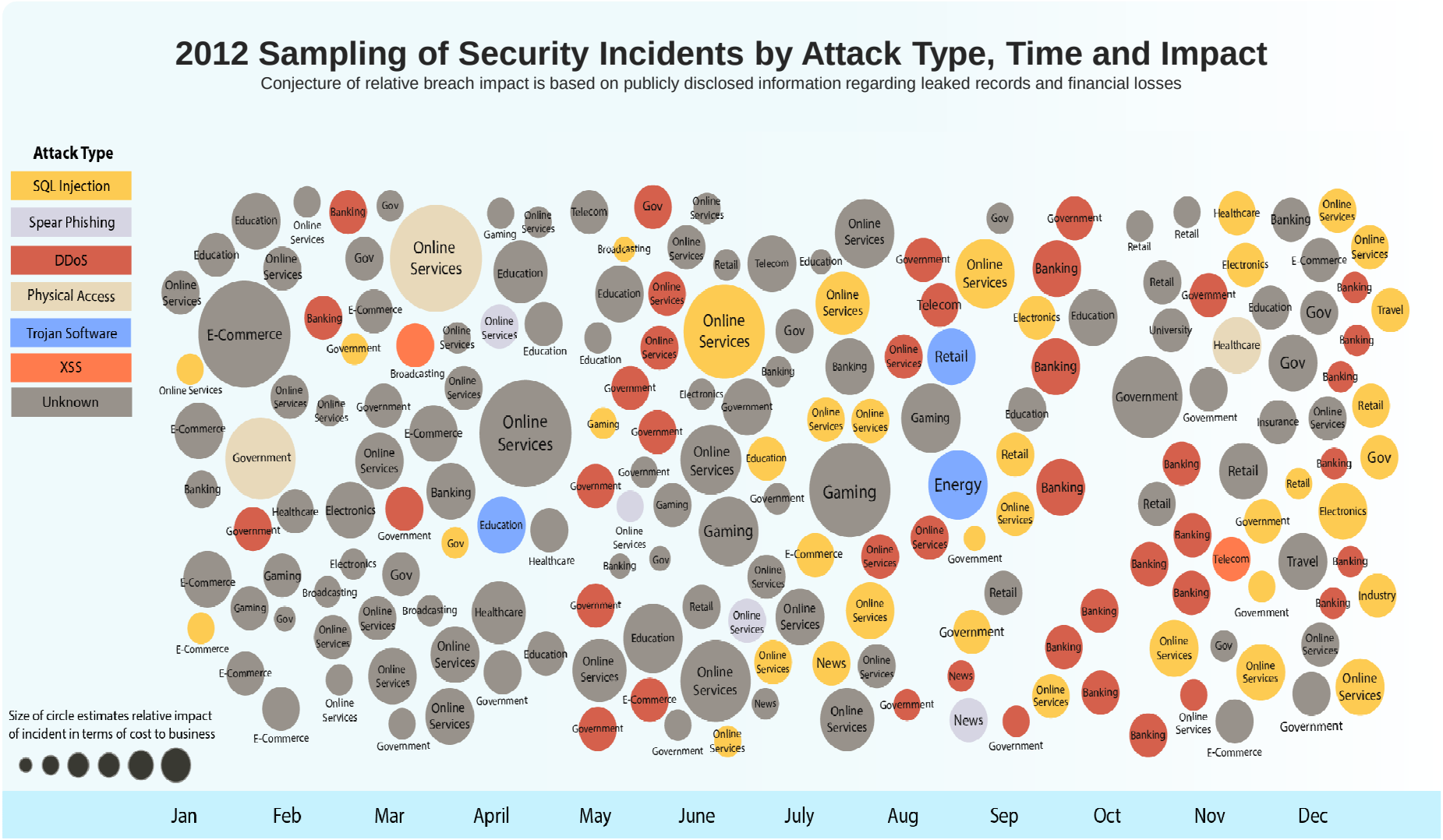
CYBER-CRIME

2011: “The year of the targeted attack”



Source: IBM X-Force® Research 2011 Trend and Risk Report

2012 : a massive rise in advanced and other attacks



Hacking optimization in action …

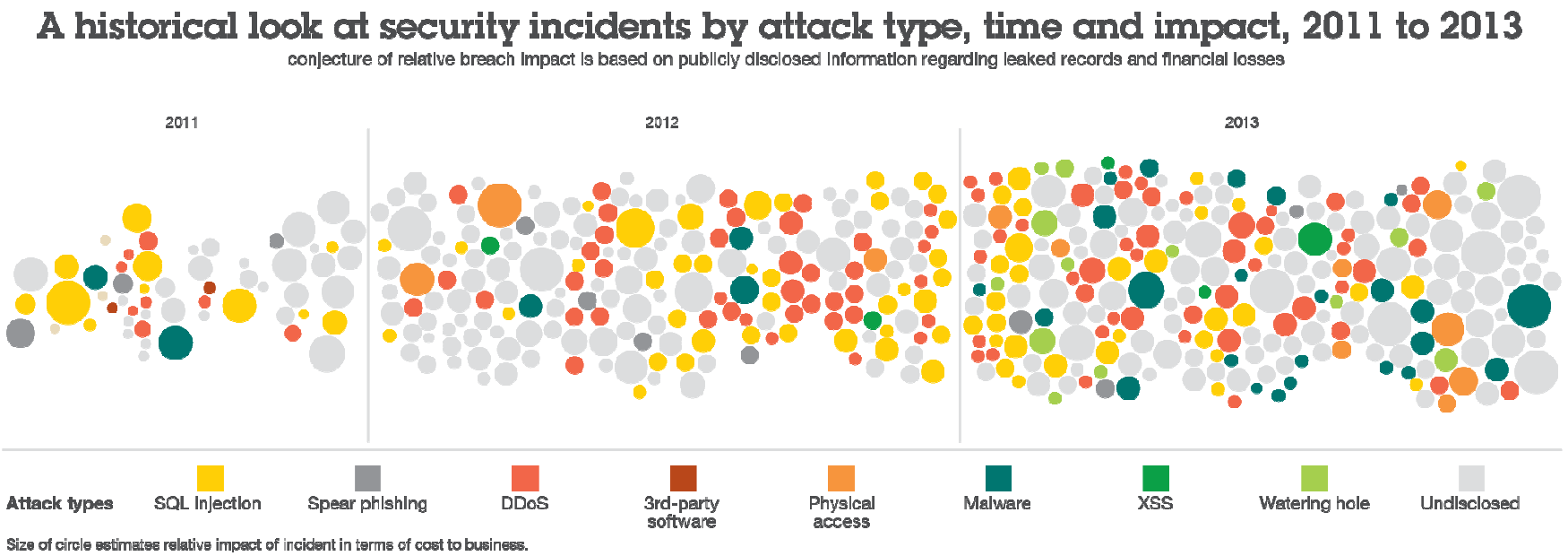


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

Not *If*, but *When*

- Breaches are taking longer to discover
- Breaches are not being discovered internally (92%)

Figure 4. Breach discovery timeframe by percent of records

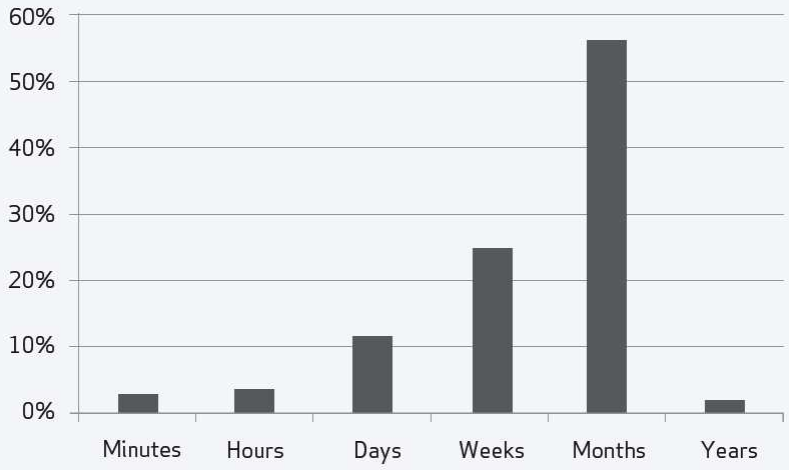
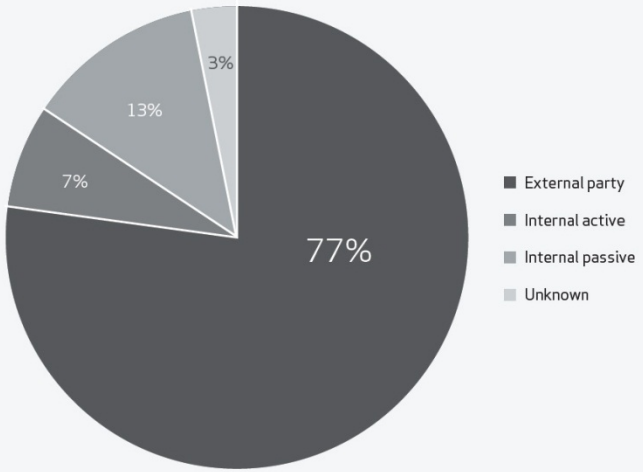
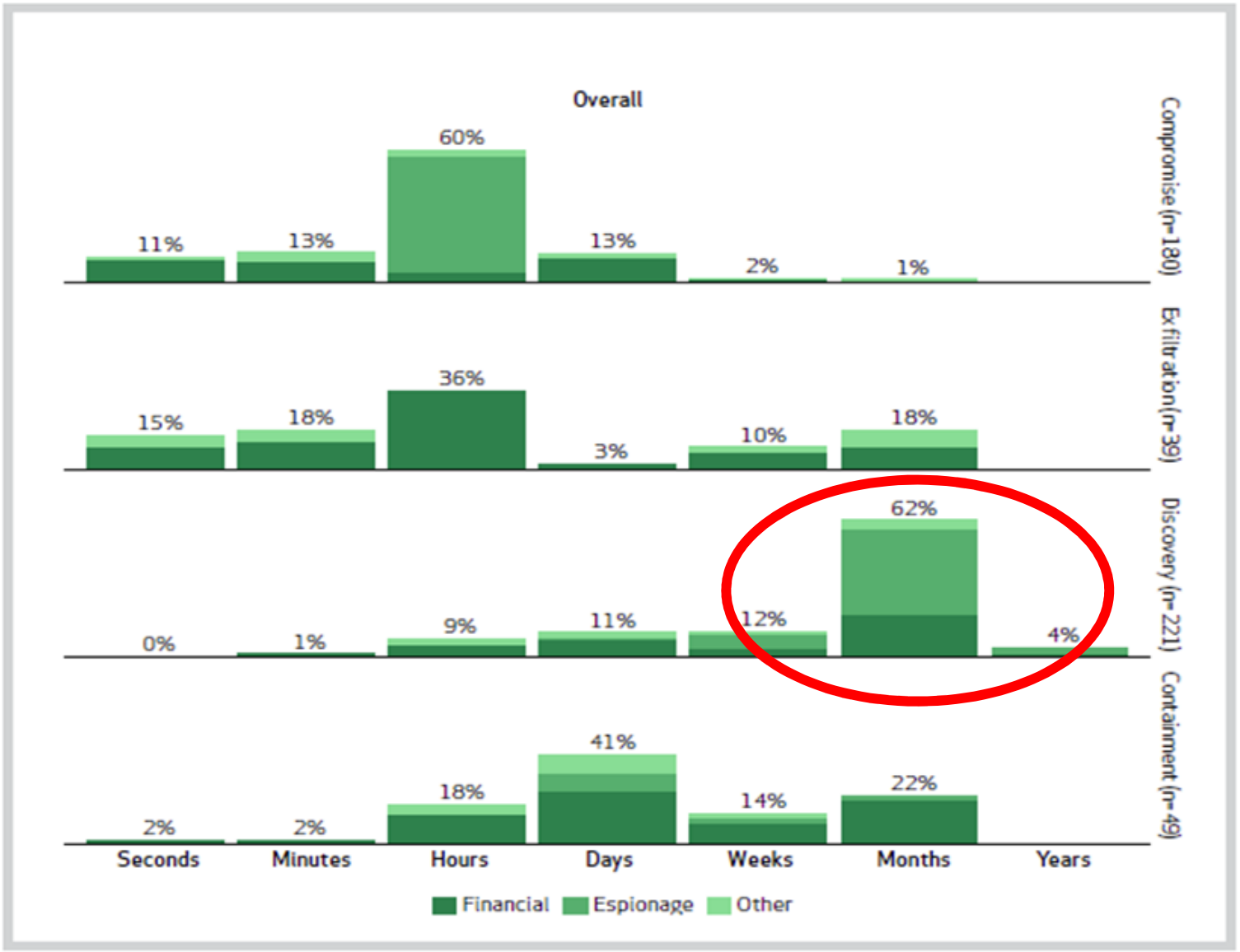


Figure 5. Simplified breach discovery methods by percent of records



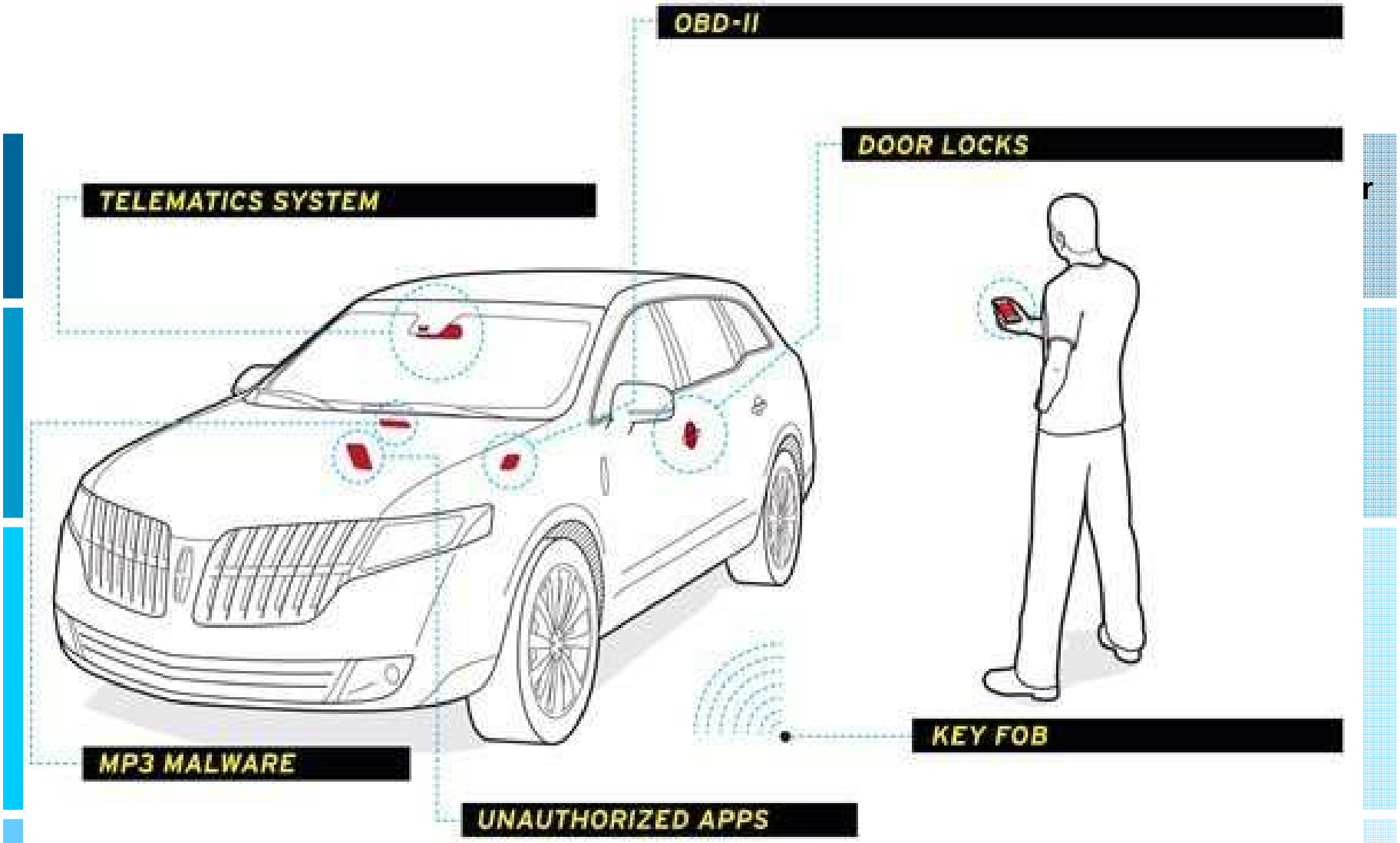
Charts from Verizon 2011 Investigative Response Caseload Review

70% of the hacks detected by outside … Months after



source [Verizon 2011 Investigative Response Caseload Review]

The attack surface is growing at an exponential rate



Security challenges are impacting business agility

External threats

Sharp rise in external attacks from non-traditional sources

- Cyber attacks
- Organized crime
- Corporate espionage
- State-sponsored attacks
- Social engineering

Internal threats

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employee actions
- Mix of private / corporate data

Compliance

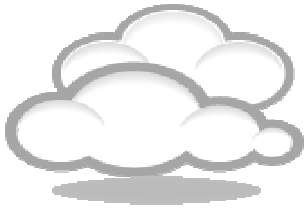
Growing need to address an increasing number of mandates

- National regulations
- Industry standards
- Local mandates

Impacting innovation

Mobility

Cloud / Virtualization



Social Business

Business Intelligence

The “Barbarian” is inside the gate

Operator Error
60%

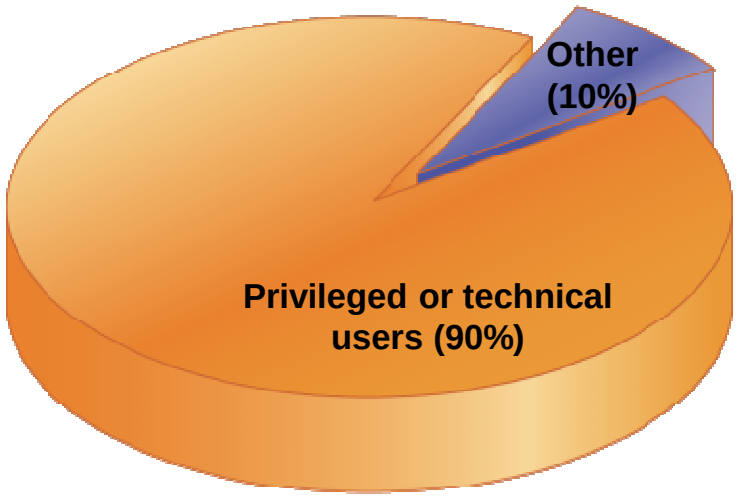
Malicious Attacks
20%

Application Failure
20%

The enemy is “us”:

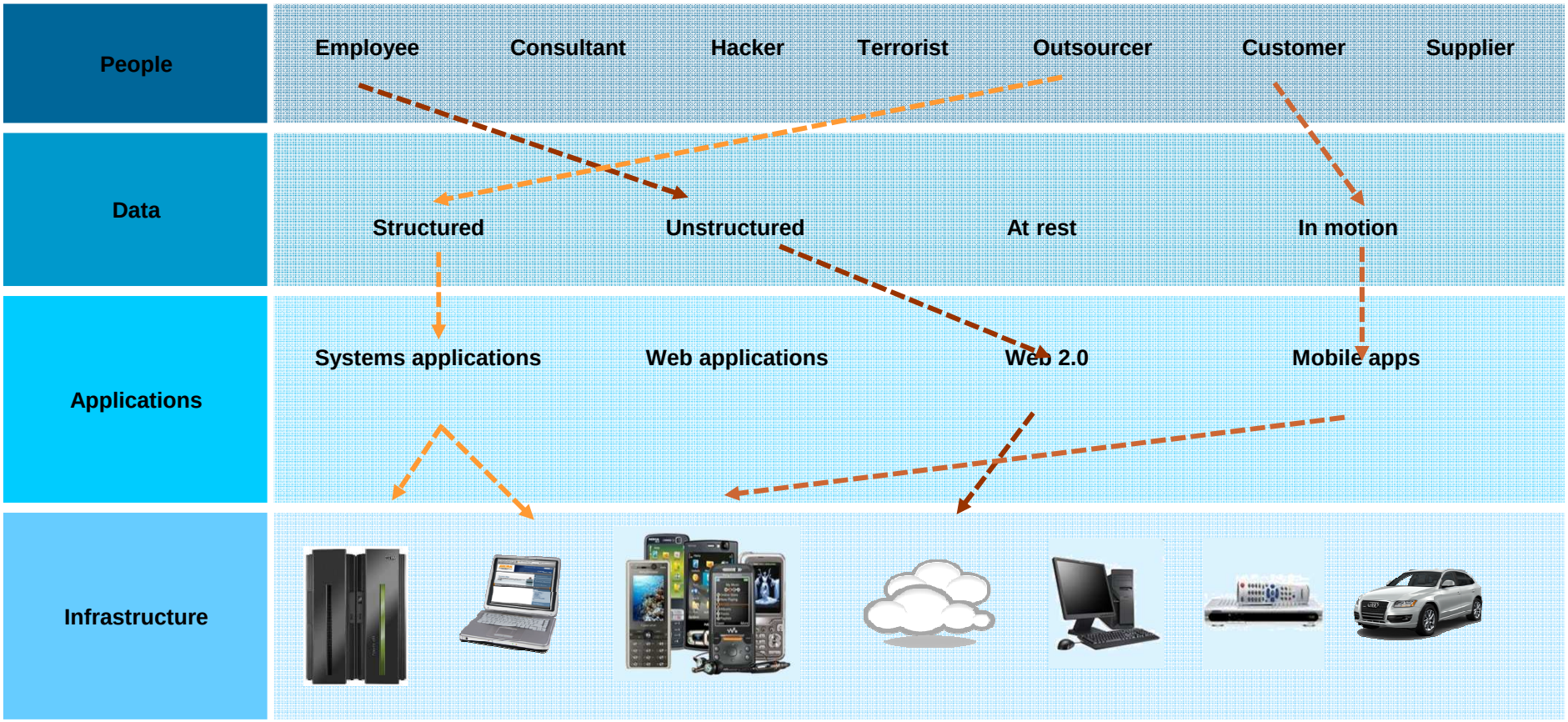
- **90% of insider incidents are caused by privileged or technical users**
- **Most are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
  - Account management process
- **Others are deliberate, due to:**
  - Revenge (84%)
  - “Negative events” (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day

Who Causes Internal Incidents?



Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

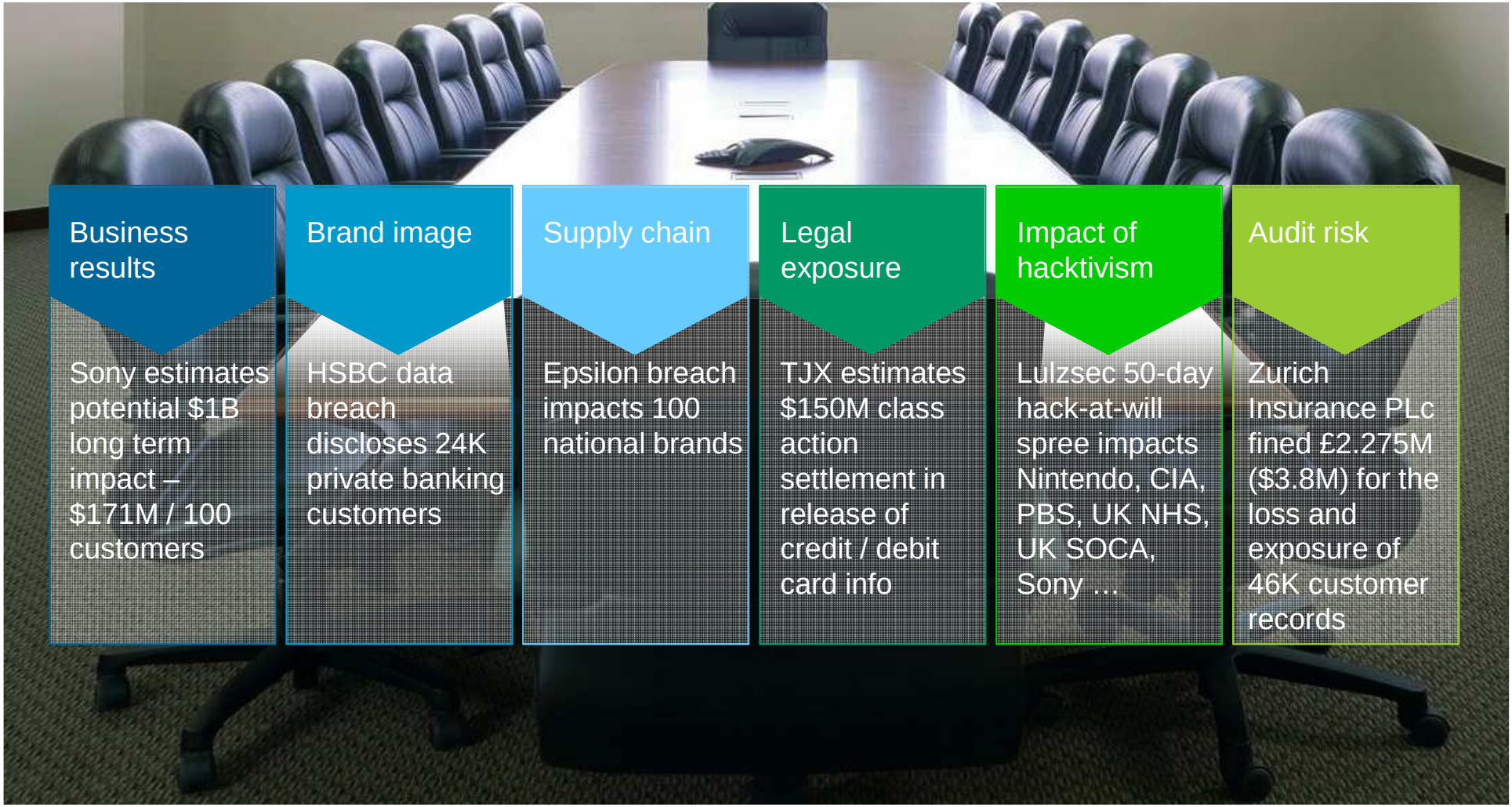
Change 3: The attack surface for a typical business is growing at an exponential rate



Change 4: The impact of a breach is now not contained to IT, but reverberates across the corporation

	CEO	CFO/COO	CIO	CHRO	CMO
CxO priority	Maintain competitive differentiation	Comply with regulations	Expand use of mobile devices	Enable global labor flexibility	Enhance the brand
Security risks	Misappropriation of intellectual property Misappropriation of business sensitive data	Failure to address regulatory requirements	Data proliferation Unsecured endpoints and inappropriate access	Release of sensitive data Careless insider behavior	Stolen personal information from customers or employees
Potential impact	Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

The Result: Security is becoming a board room discussion



Pressure: CEOs don’t look good in orange

1 - 2 years	**Escaping from prison**
3 - 5 years	**Kidnapping involving Ransom**
11 - 14 years	**Second Degree Murder**
10 - 20 years	**Fraudulent SOX Certification**
20 - 25 years	**Hijacking**

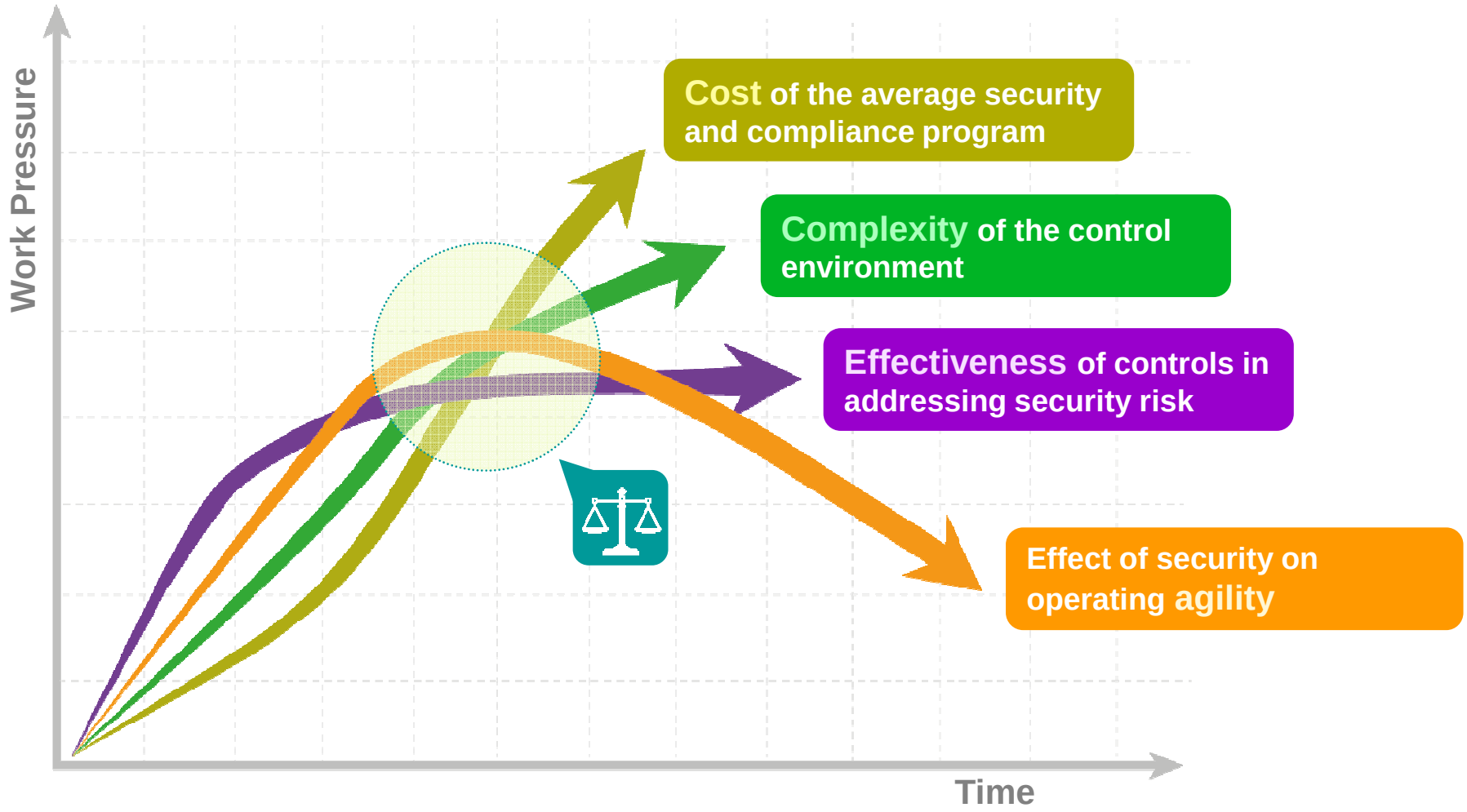
What are the security challenges?

***Cost** of "Effective Security" has been rising faster than our budgets*

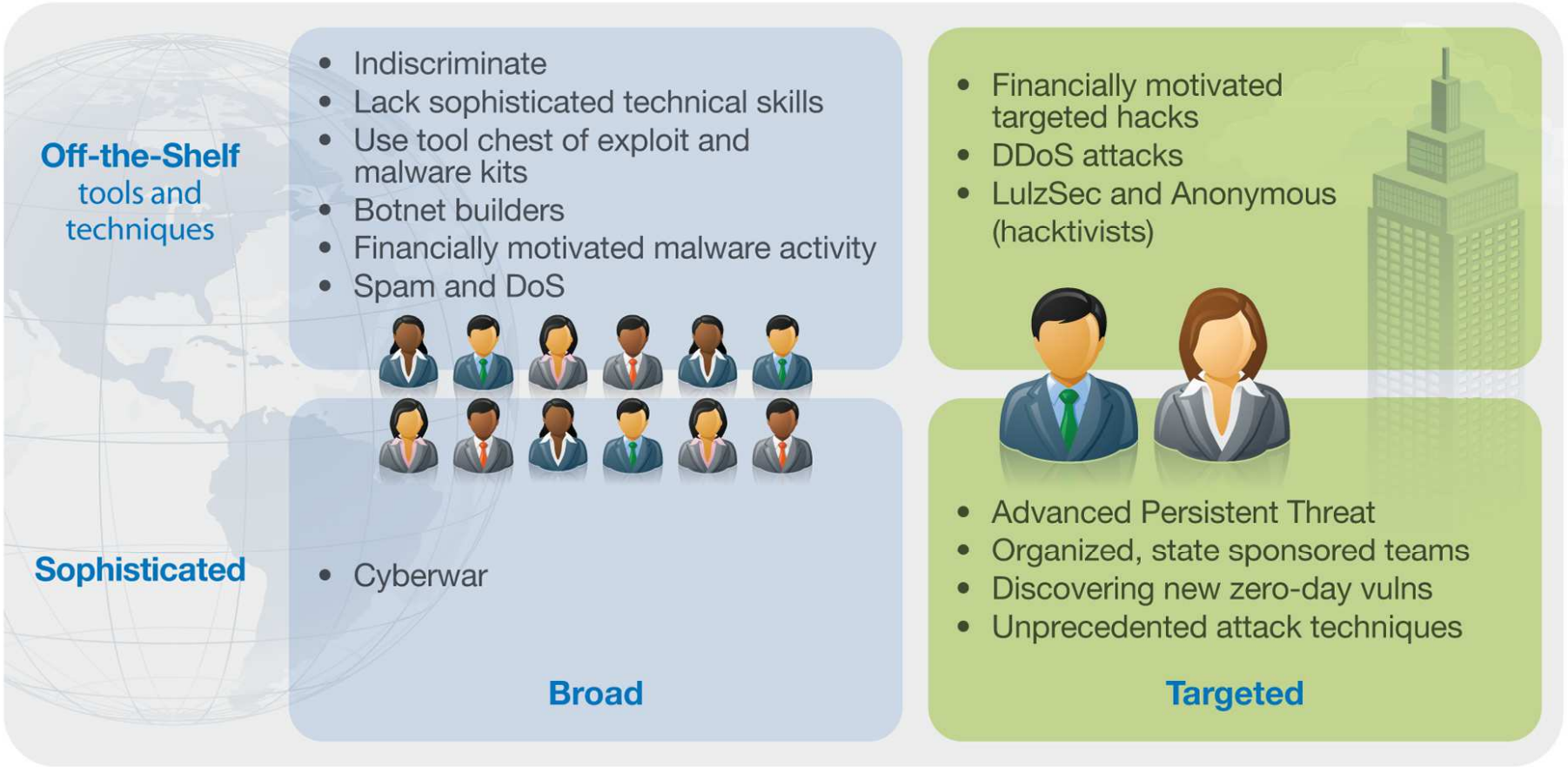
*While **Compliance** continues to be the hammer with which we can secure funding – spending results in more point products to solve more point problems*

*The **Complexity** of the security problem and the solution makes it difficult to know how much security is "good enough"*

The IT security challenge: manage cost, decrease complexity, improve effectiveness and assure agility.

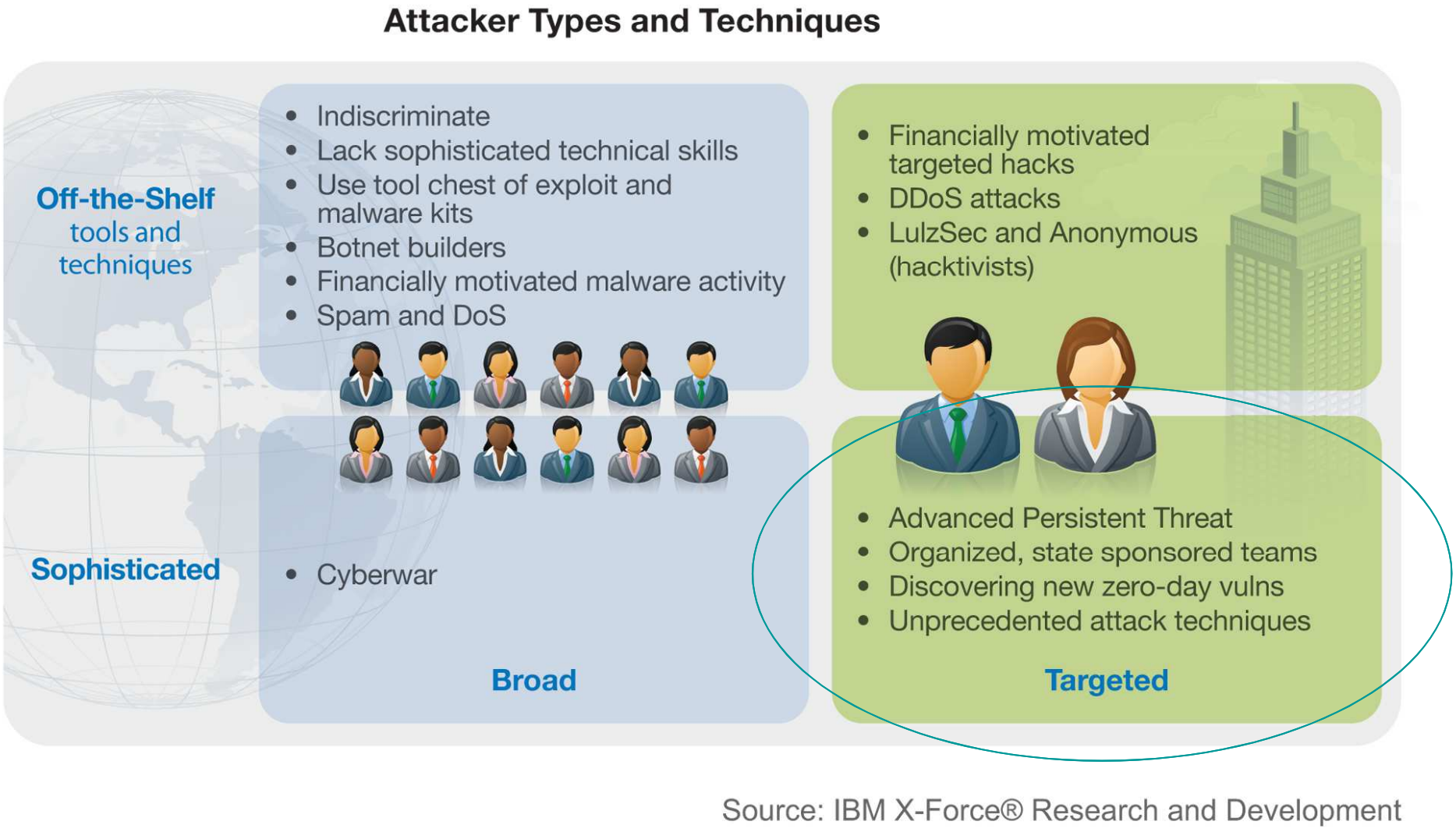


Who is attacking?



Source: IBM X-Force® Research and Development

Who is attacking ?



Source: IBM X-Force® Research and Development

Amateurs study Cryptography: Professionals study Economics

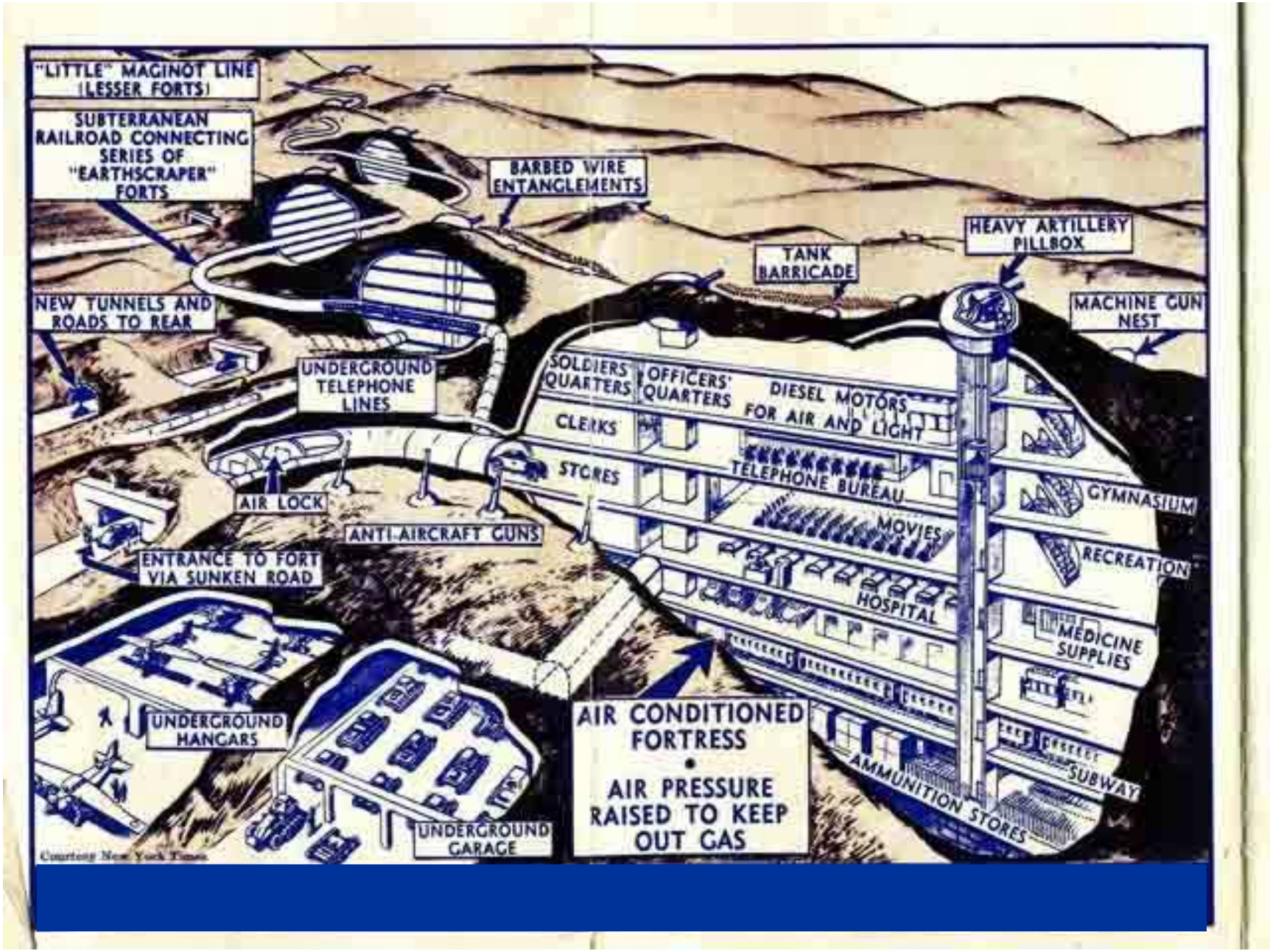
The Computer Criminals Business model :

Amount of revenue VS Cost of development /deployment

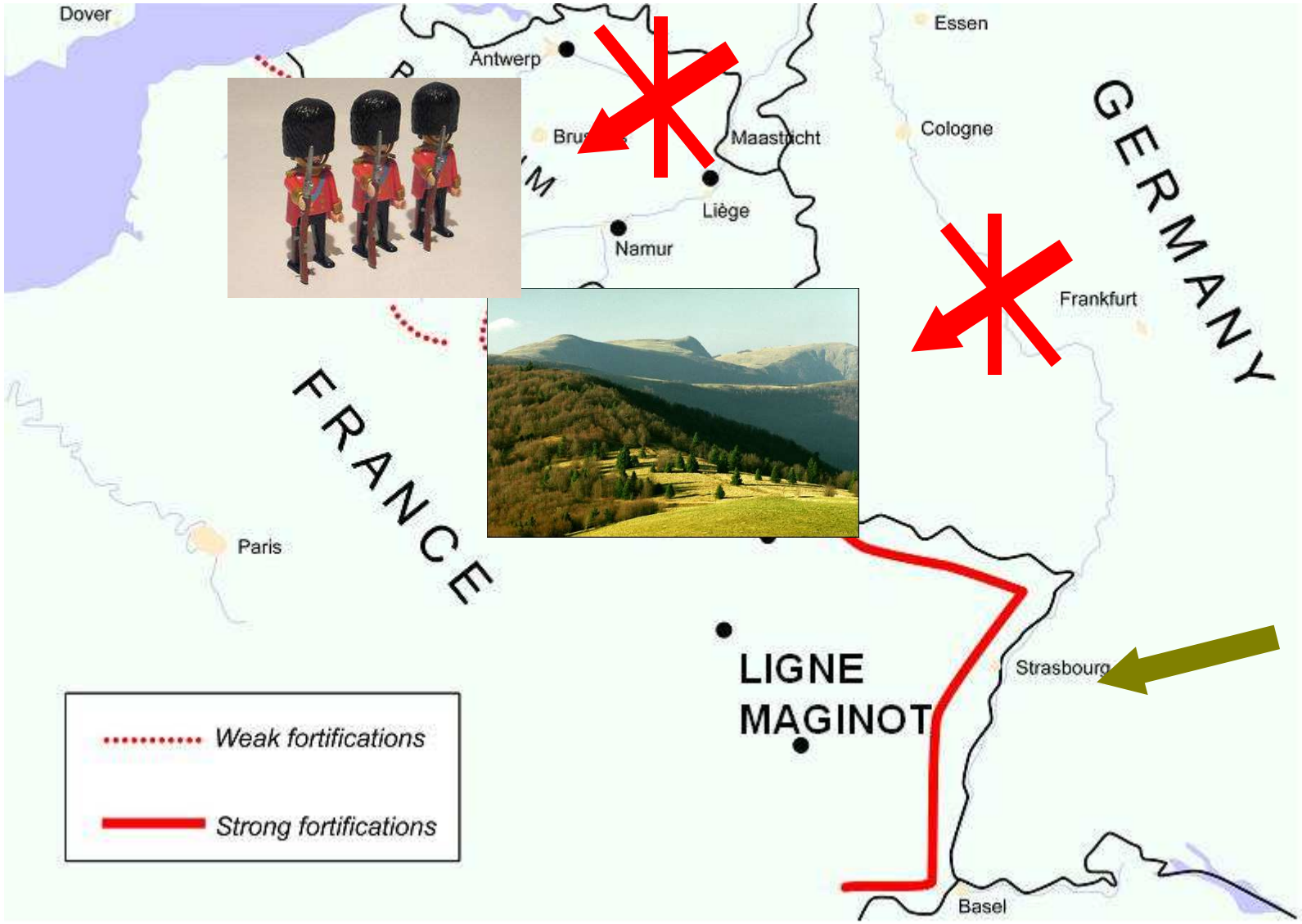
Need to understand the context

- “The rapid discovery of a breach is key to minimizing the damage of a targeted attack, but **most organizations do not have adequate breach detection** capabilities.”
- “Since perfect defenses are not practical or achievable, organizations need to augment vulnerability management and shielding with more-effective **monitoring**.”
- “The addition of **context, such as user, application, asset, data and threat**, to security event monitoring will increase the likelihood of early discovery of a targeted attack.”
- “We need to get better at discovering the **changes in normal activity patterns** that are the early signal of an attack or breach.”

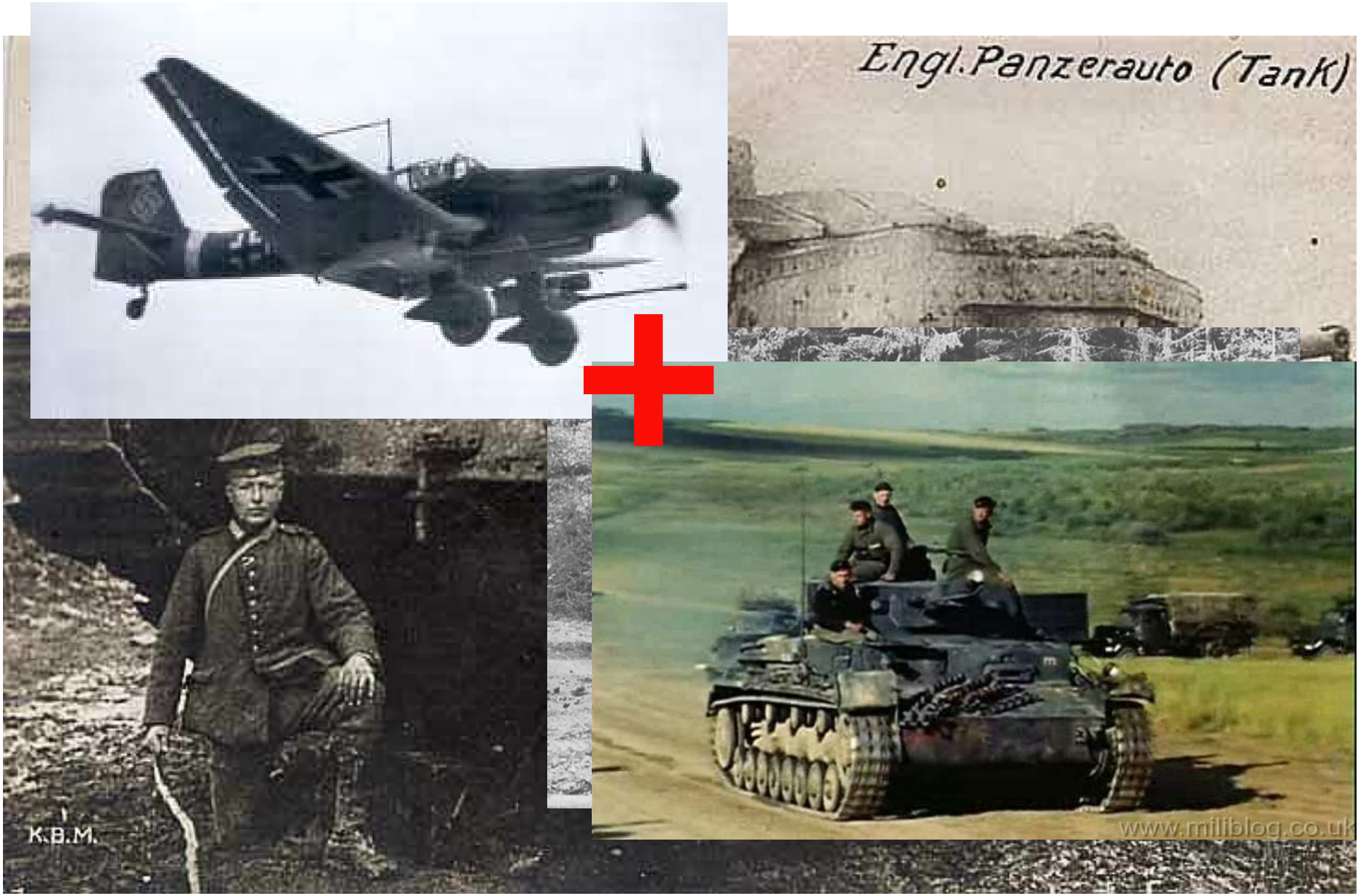
An unbeatable defense



The defense context & risk analysis



The technology changes the context & the impacts



Strategy failure analysis

- New context
- The strategic informations were known …
- There were not aggregated /correlated
- There were not no global analysis
- Result: no quick and efficient counter measure

Today common strategy : two factor again !

Techniques used by attackers are bypassing traditional defenses

Advanced

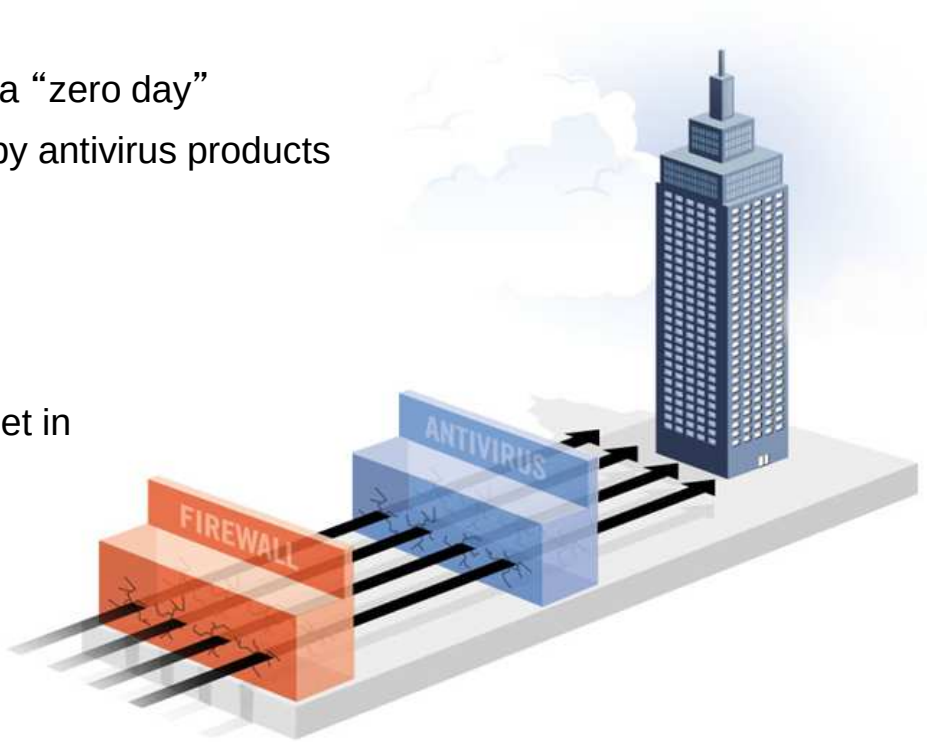
- Using exploits for unreported vulnerabilities, aka a “zero day”
- Advanced, custom malware that is not detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in
- Resistant to remediation attempts

Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are actually “out to get you”



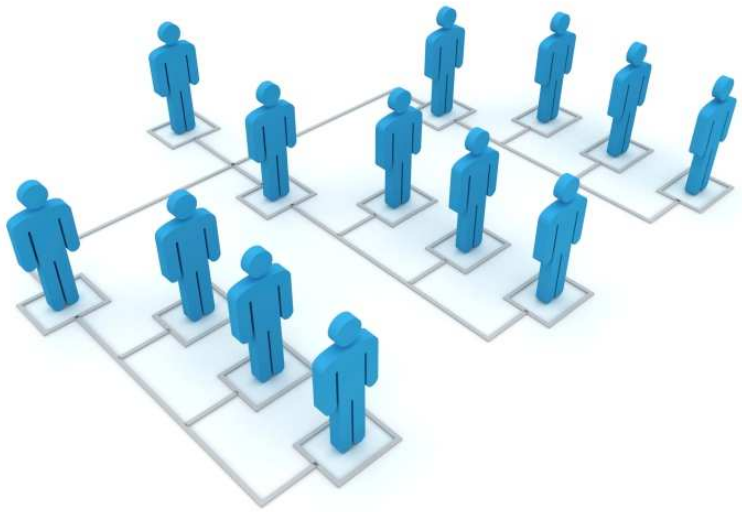
These methods have eroded the effectiveness of traditional defenses including firewalls, intrusion prevention systems and antivirus - ***leaving holes in the network***

Internet Intelligence Collection

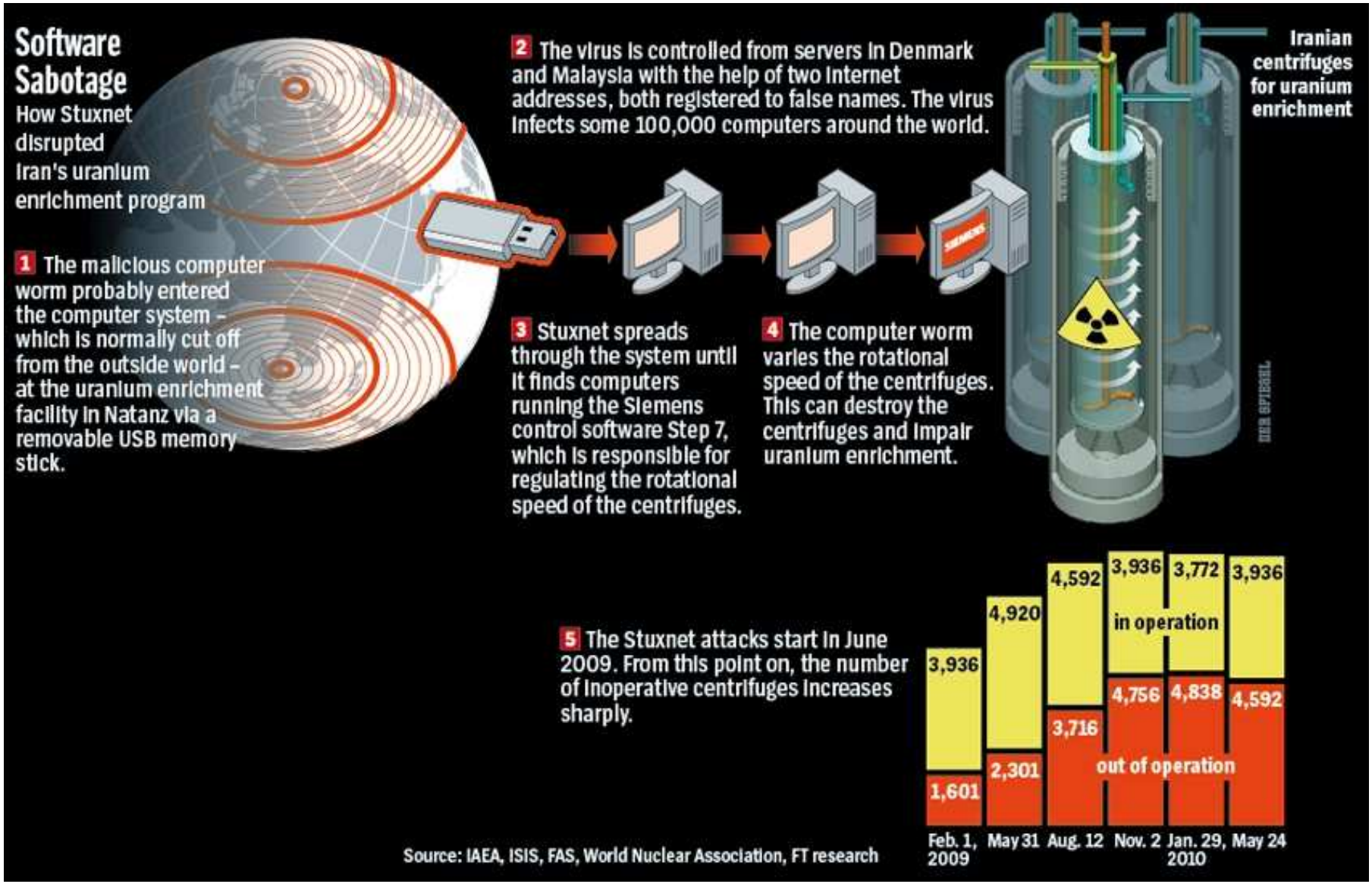
- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?
  - Write index cards with names and titles

- Search for Linkedin, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart

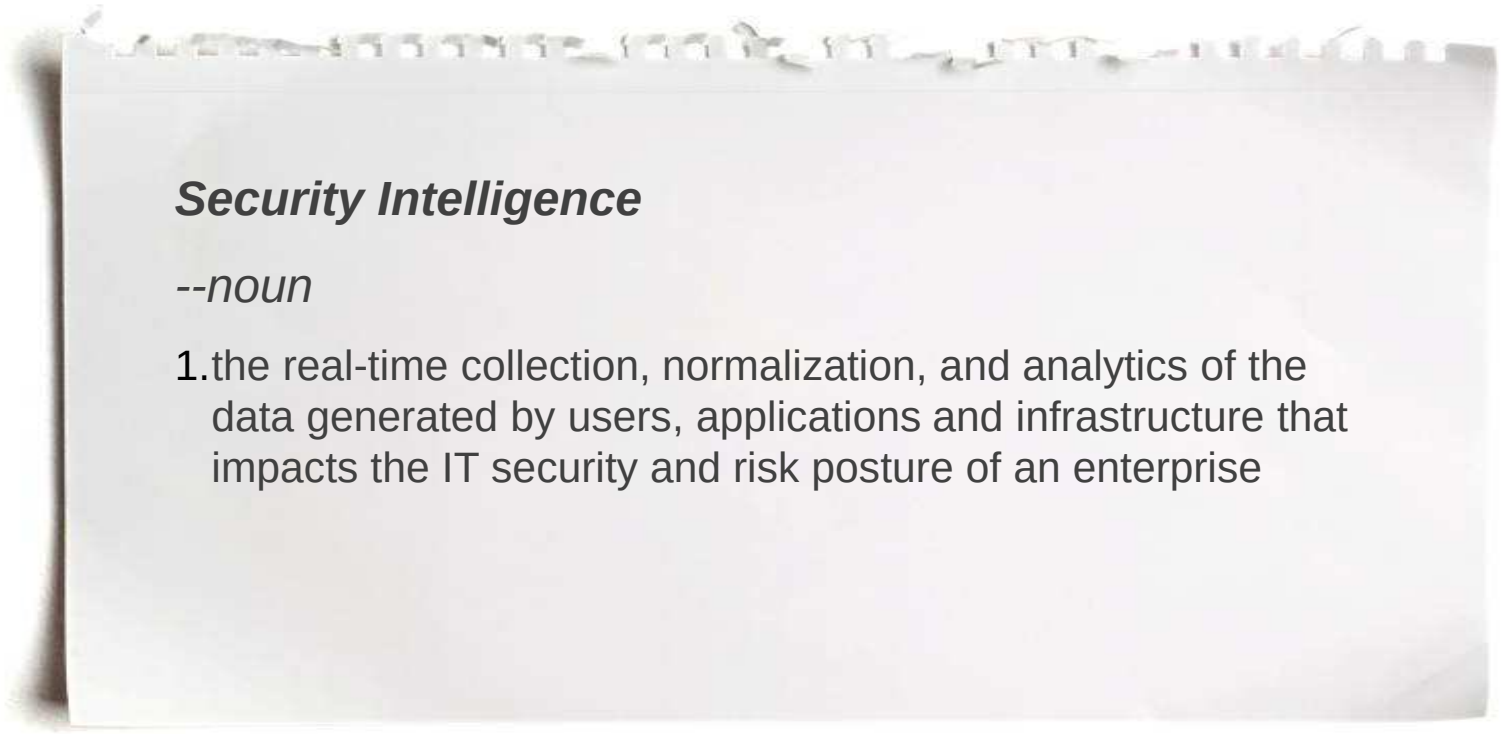
- Who works with the information we'd like to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?



Suxnet a targeted Attack

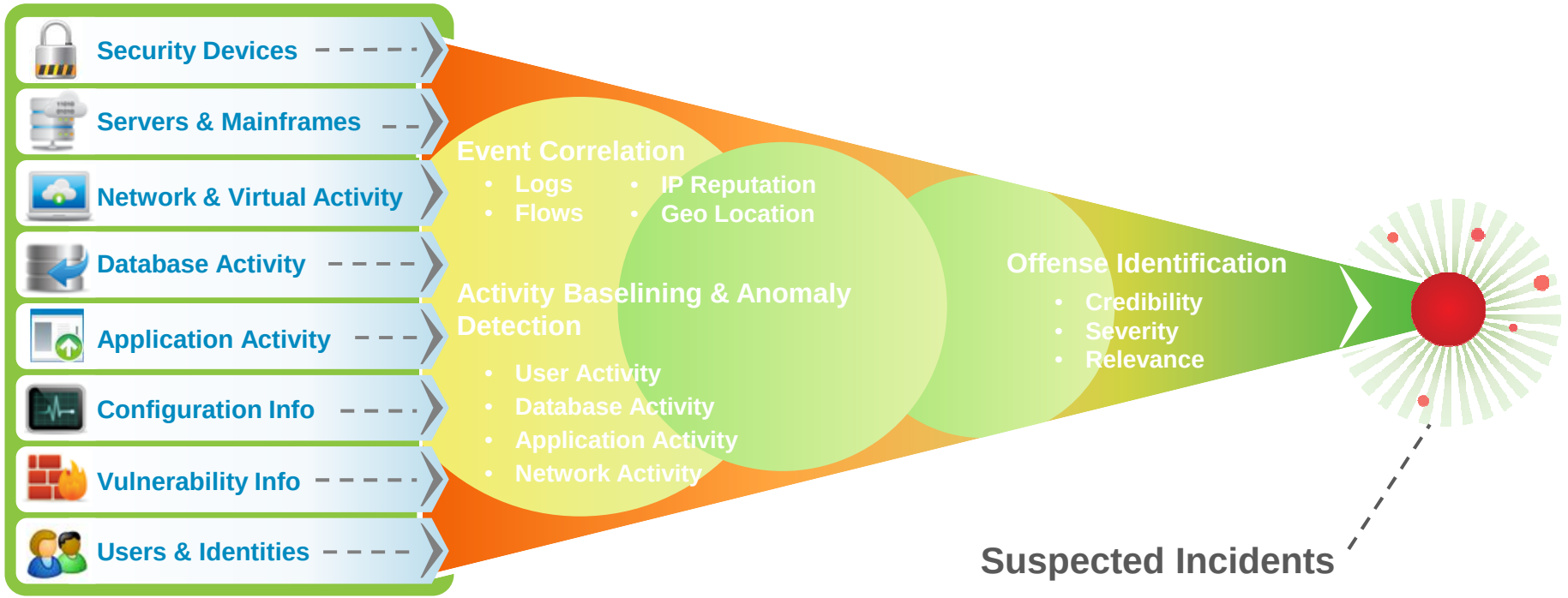


What is Security Intelligence?



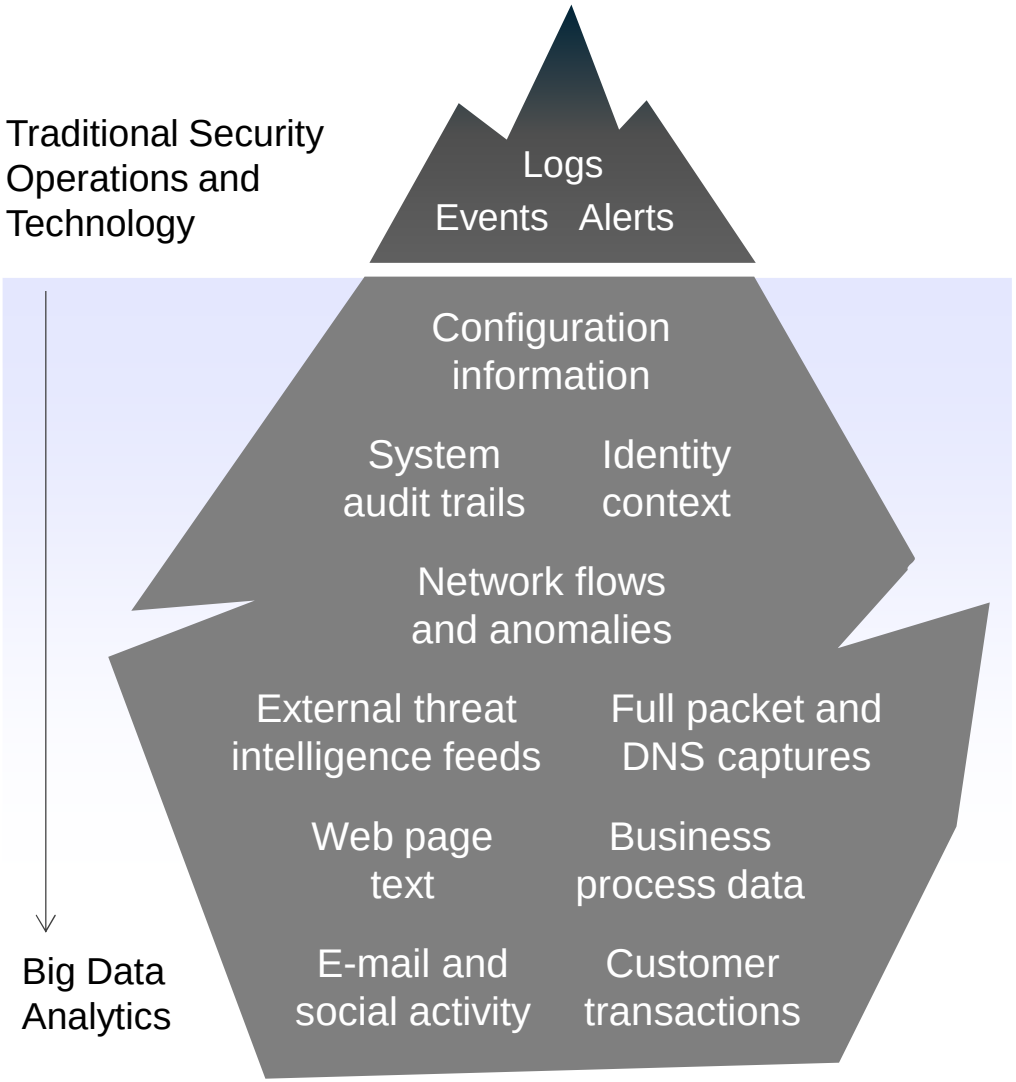
Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

Context and Correlation Drive Deep Insight



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Very good but could be improve



New Considerations

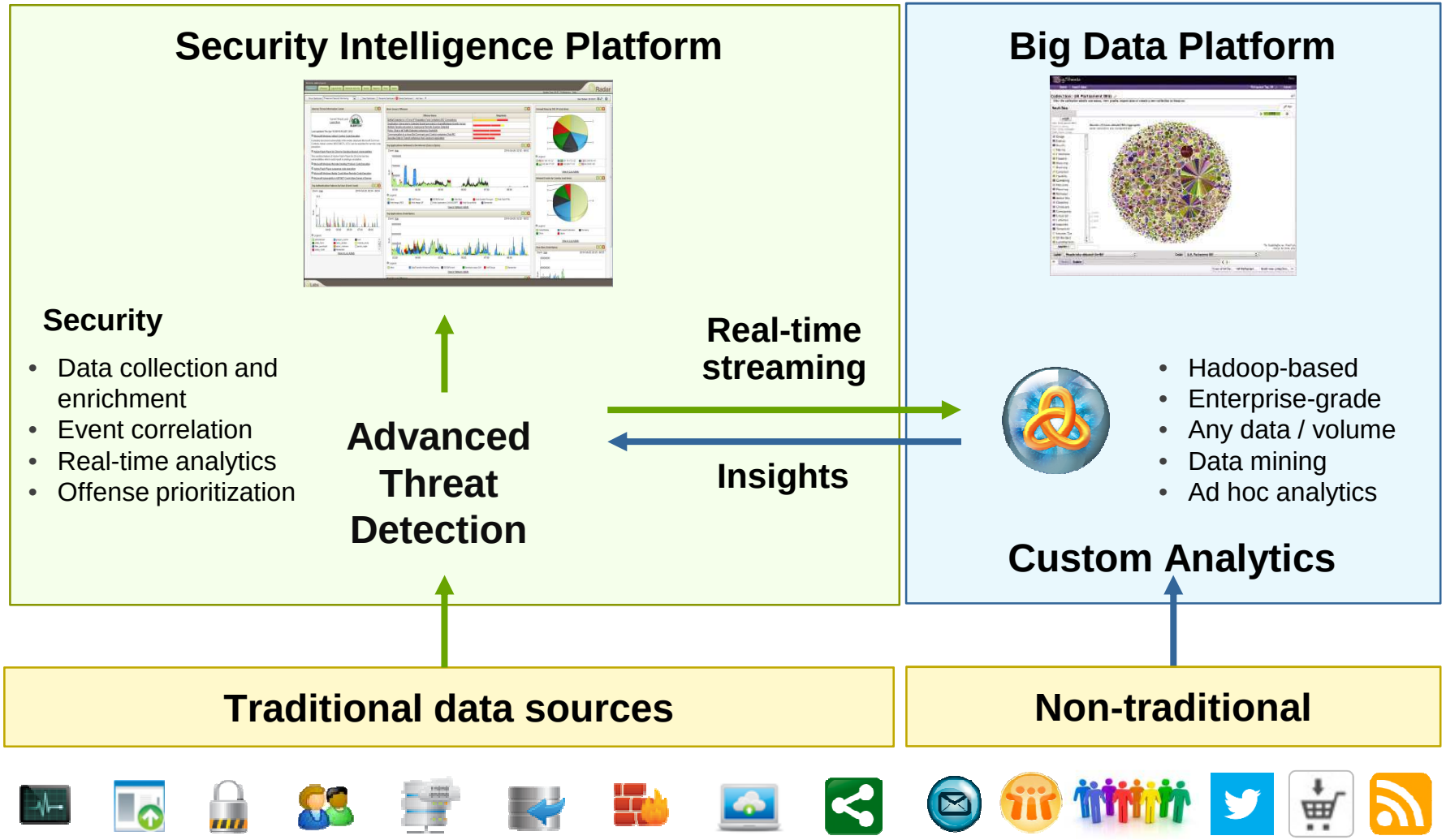
Collection, Storage and Processing

- Collection and integration
- Size and speed
- Enrichment and correlation

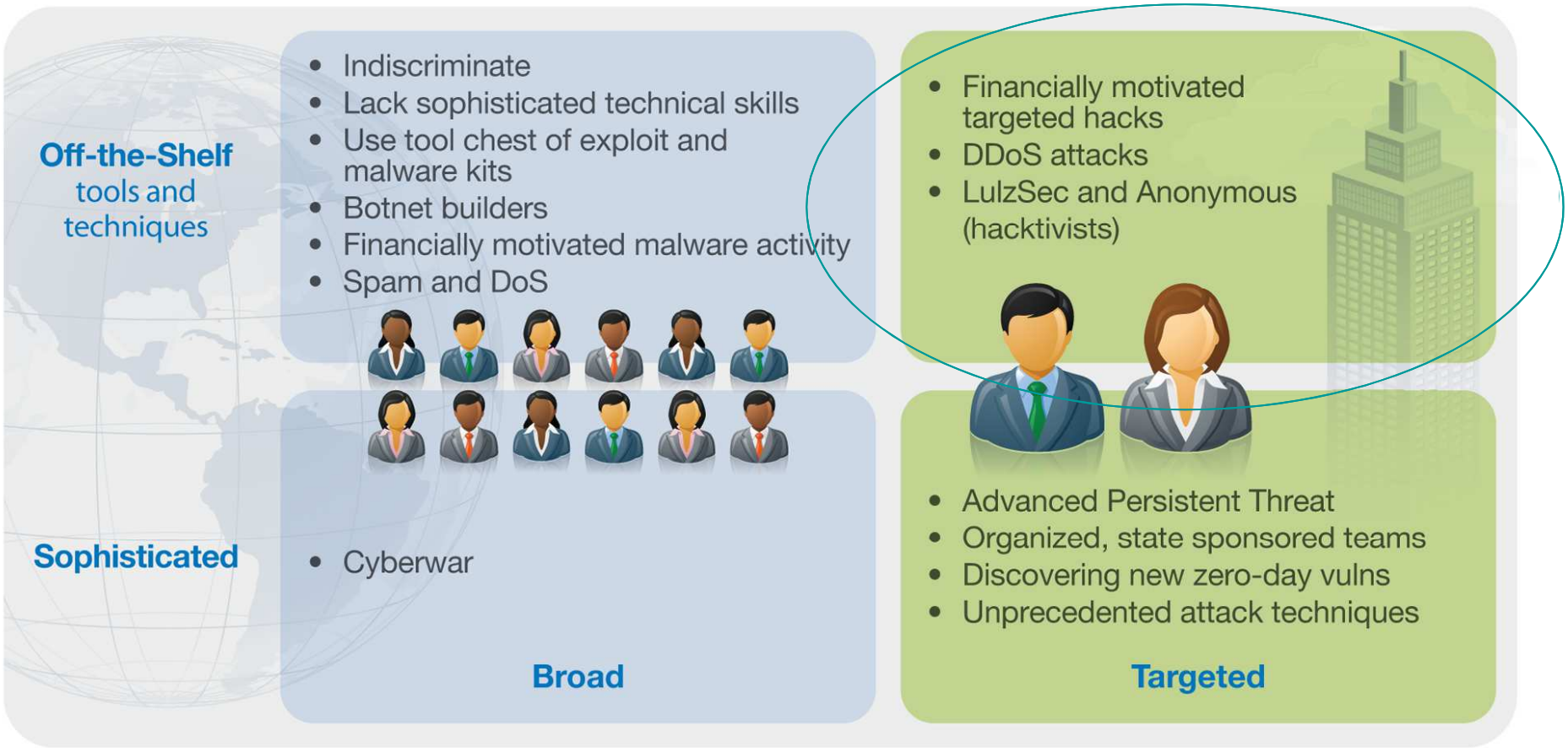
Analytics and Workflow

- Visualization
- Unstructured analysis
- Learning and prediction
- Customization
- Sharing and export

How? By integrating security dashboard with Big data



Who is attacking?



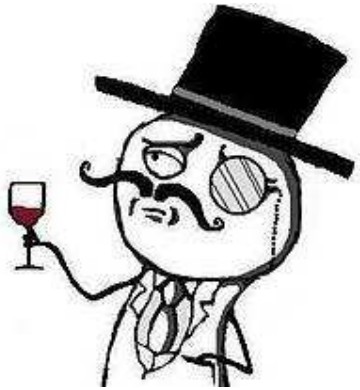
Source: IBM X-Force® Research and Development

Hacktivists are politically motivated

A member of Anonymous at the Occupy Wall Street protest in New York*

ANONYMOUS

One self-description is:
"We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."**



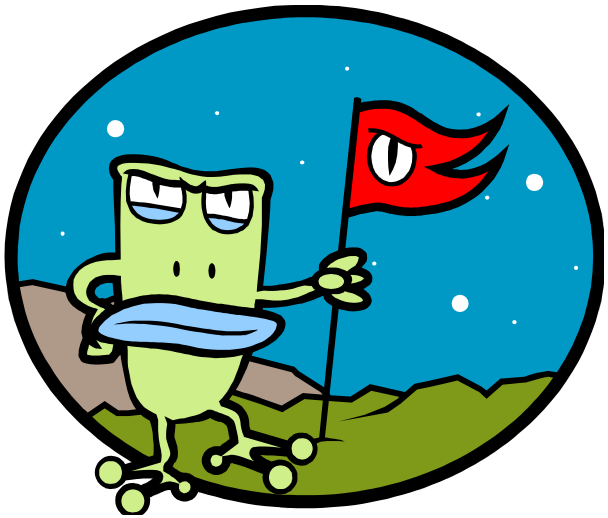
Lulz Security logo

"The world's leaders in high-quality entertainment at your expense."

*Source: David Shankbone

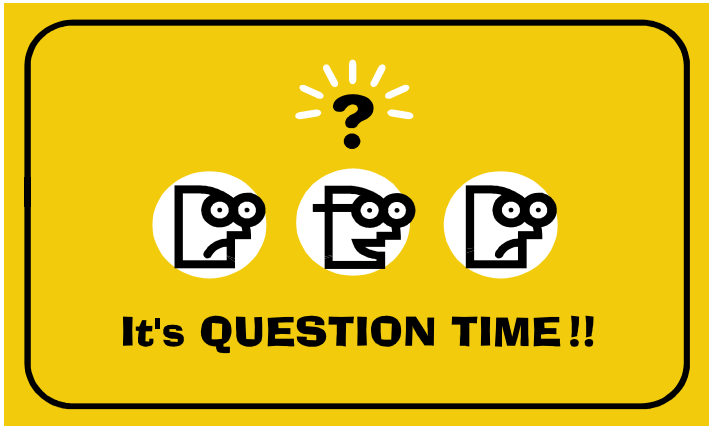
**Source: Yale Law and Technology, November 9, 2009

The New frontier

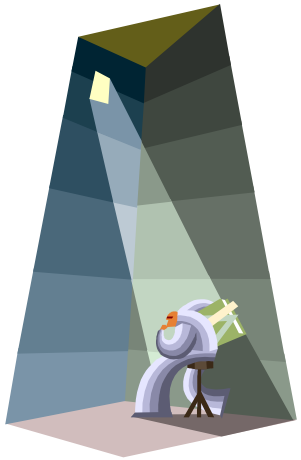


New regulations imply Stronger IT security strategy, plans and capabilities.

Why 10 to 20 are key numbers for the security Business ?



And the answer is:

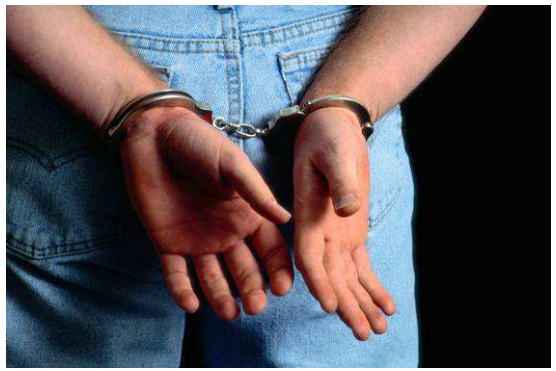


- Prison sentence of 10 years to 20 year for CEO's and CFO's to failure comply to
- 10 to 20% of IT budget increase to comply to

Sarbanes-Oxley Act ……

Putting this into context…

1 - 2 years	Escaping from prison
3 - 5 years	Kidnapping involving Ransom
10 - 20 years	**Fraudulent SOX Certification**
11 - 14 years	Second Degree Murder
20 - 25 years	Hijacking



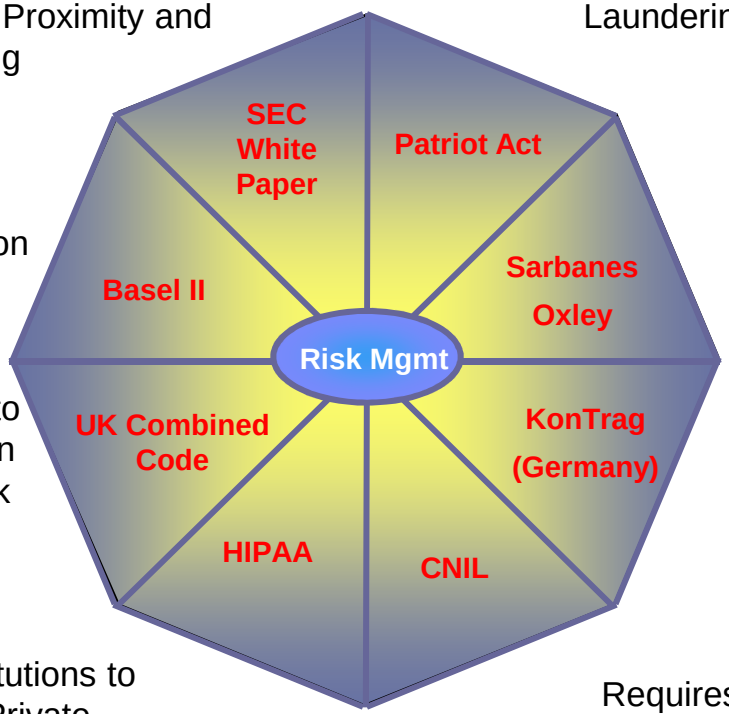
Market speak: Recent world events and corporate scandals have forever changed the global risk landscape...

SEC/OCC/Fed Draft Regulations Sets New Standards for Data Center Proximity and Industry Testing

New Draft Accord Requires Financial Institutions to Report on "Operational Risk"

Requires Companies to Report to Shareholders all Information on Financial and Operational Risk Management Controls

Requires Health Care Institutions to Safeguard and Keep Private "Individually Identifiable Patient Healt Information"

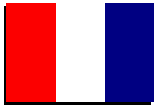


Enacts "Know Your Customer" Anti-Money Laundering Regulations

Sets Higher Financial Reporting and Governance Standards for Corporate Boards and Executives

Requires Directors to Establish Risk Management Supervisory Systems and Report "Control" Information to Shareholders

Requires Companies to Safeguard and Keep Private individual Information

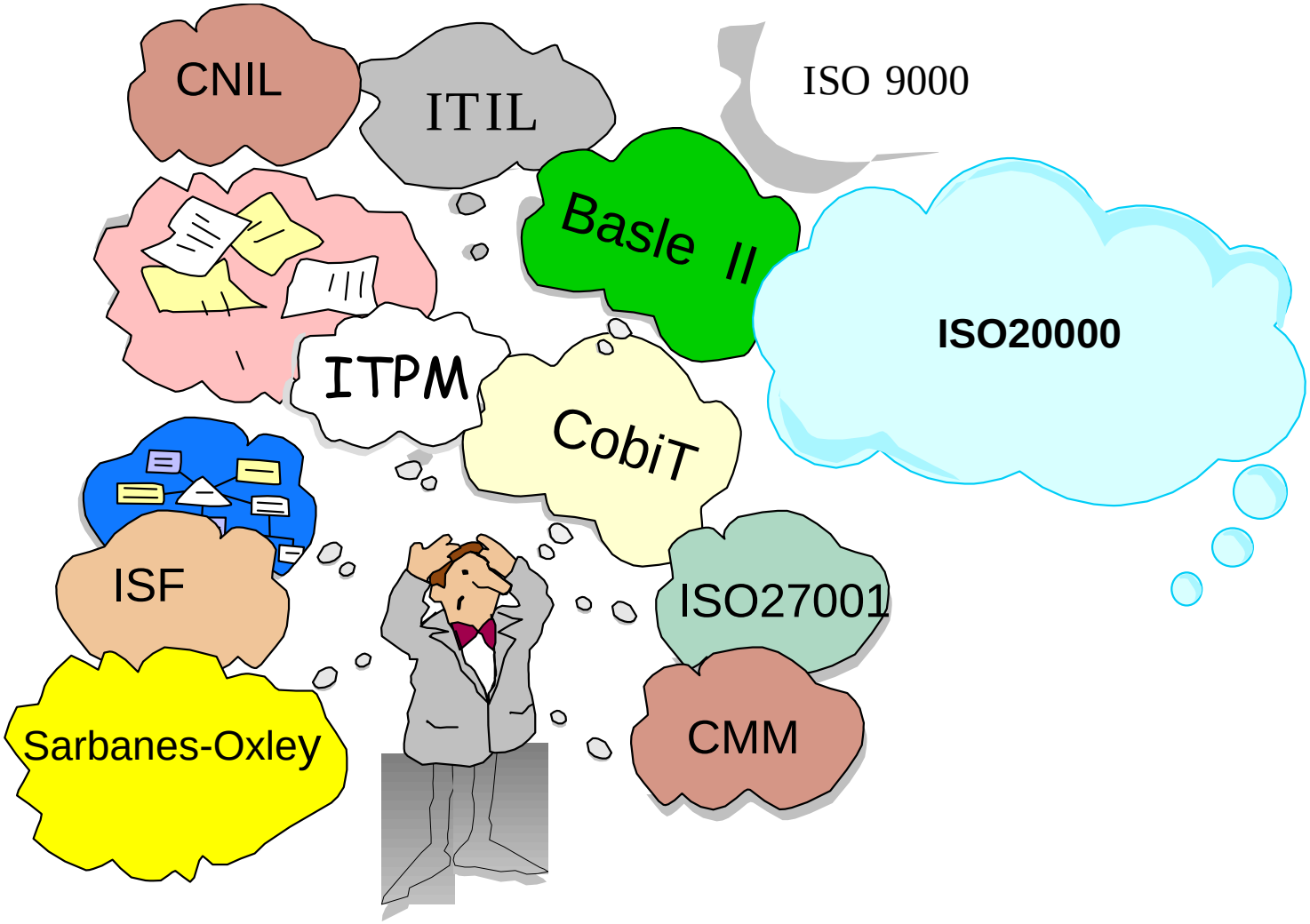



Nearly the same or worse in Europe !!!!

Some regulations the French's companies MUST be compliant :

- Décret sur l'hébergement des données de santé (Safeguard and Keep Private Individually Identifiable Patient Health Information)
- Proposition de directive sur la « perte » de données personnelles (data breach notification)
- Target 2 : European control of big fund transfers
- Solvency 2 : Insurance risk control & assessment
- IAS/IFRS : International accounting standard
- Law for trust in e commerce (LCEN)
- CNIL protecting individual data
- Bâle 2 (Basel II)
- Sarbanes-Oxley Act (if US business)
- Archivage réglementaire (legal archiving)
- ……

The CIO new challenges : compliance to security laws and standards



The companies security needs have to be addressed in a Top Down approach

- Security is a must to stay in the business it becomes a CEO's and CFO's concern .
  - Security needs relate to regulations
  - Regulations must be understood
  - Auditors have to be convince
- Auditors care :
  - Process First
  - Metrics Second
  - and finally Tools

Auditors questions

How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the IT?

How do you know your private customer data is encrypted?

Do you know if administrators are abusing privileges?

Can your auditors get at the information they need?

Are you reporting consistently across the enterprise?

How do you know only authorized users are given user accounts?

How did you protect your Web services applications?

Platform Infrastructure ⟷ **Data Privacy** ⟷ **Compliance and Audit** ⟷ **Extended Enterprise**

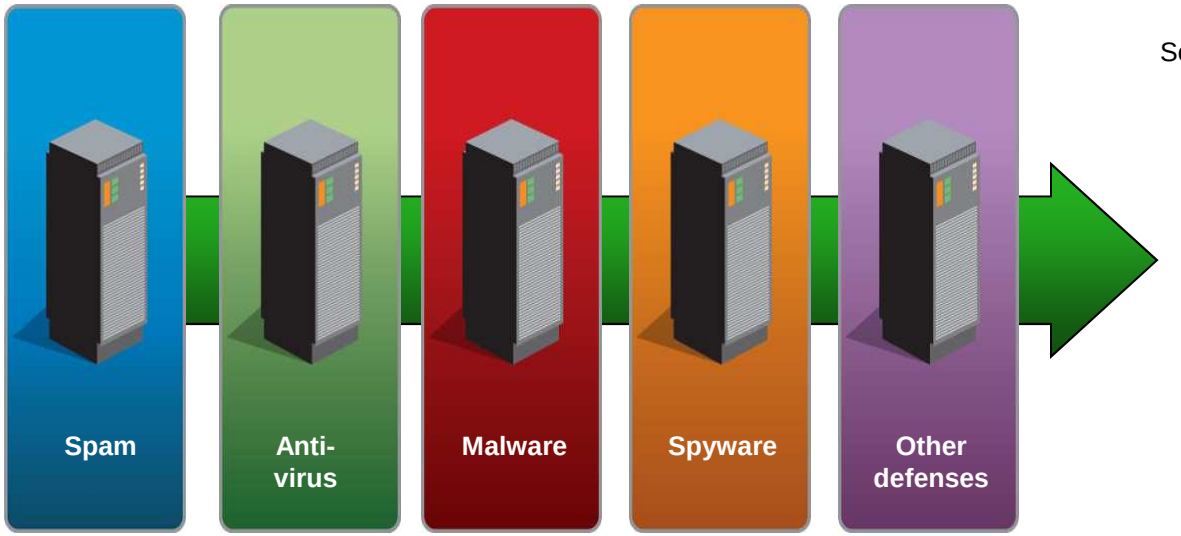
What is at Risk ?

Definition d’un risque

- Le risque désigne un **danger** bien identifié, associé à l’***occurrence*** d’un ***événement*** ou d’une série d’événements, parfaitement descriptibles, dont on ne sait pas s’ils se produiront mais dont on sait qu’ils sont susceptibles de se produire.
- La **gestion du risque** est une des phases de traitement du risque. Elle vise à en réduire les différentes formes ou sources. Dès que l'on a évalué les plus fortes vulnérabilités, on connaît mieux les causes, les objets de risque, et les conséquences pour ces vulnérabilités.
- **Prévenir** : l'action consiste à diminuer la probabilité d'occurrence du risque en diminuant ou supprimant certains des facteurs de risque.
- **Préparer la correction** : l'action consiste à diminuer l'effet du risque lorsque celui-ci intervient.

Security's silo problem and "business as usual"

A different product for each new threat

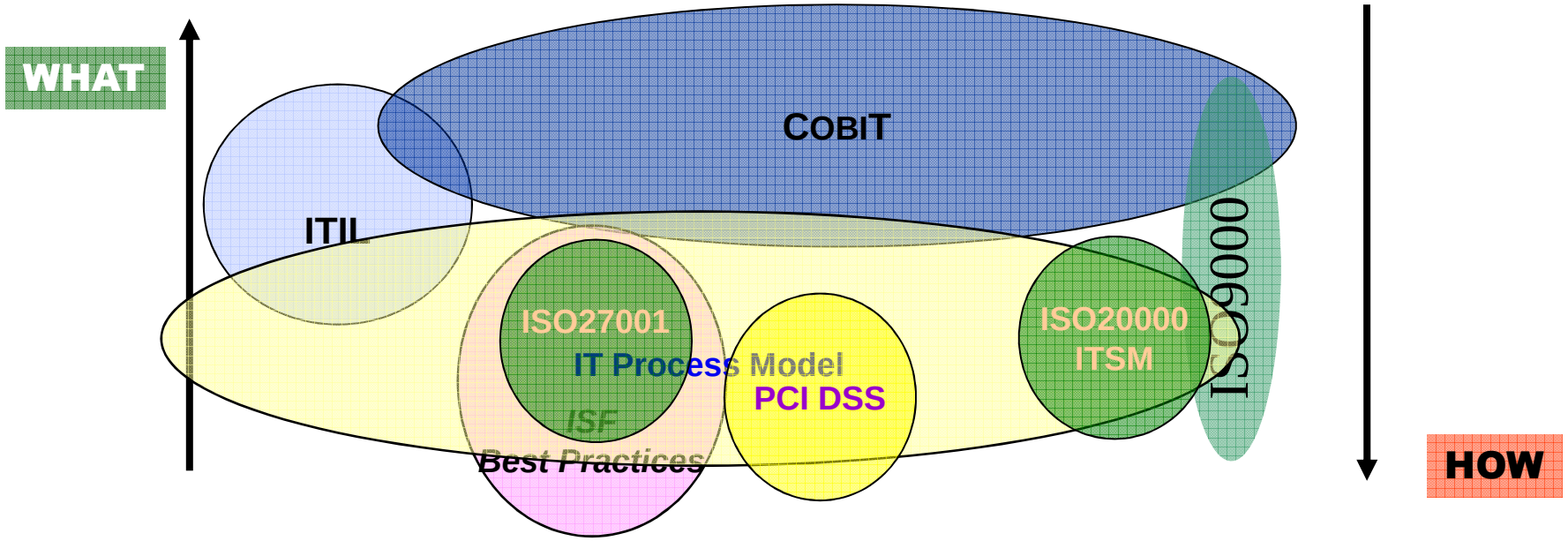


Security silos introduce:

- The need to purchase an increasing array of point products to deal with the "crisis of the day"
- Continual growth in the number of internal security staff
- The need to dedicate a larger and larger piece of IT budget to security

Key IT Governance/Security Frameworks

- COBIT®standardizes the definitions of IT controls, describes how to measure them, and the roles that are responsible for them.
- ISO 27001 (ISMS) and ISO 27002 (controls practice)
- ITIL (ISO 20000) describes best practices for organizing and running an IT organization
- PCI DSS, Payment Card Industry – Data Security Standard

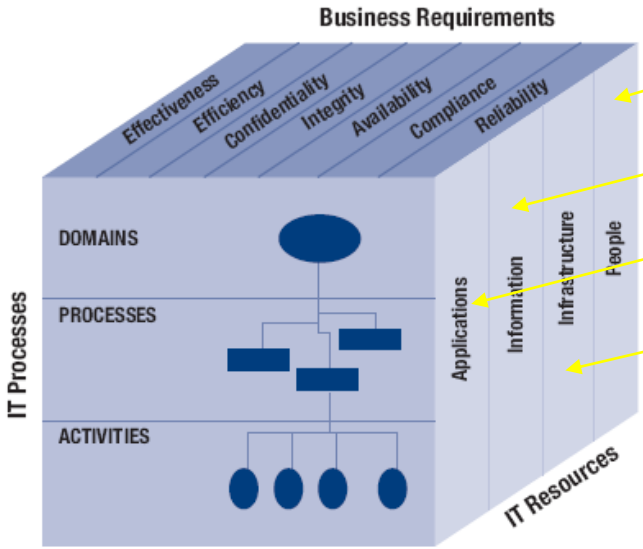


Other sources of Best Practices, Procedures and Guidelines

Une approche structurée

Control Objectives for Information and related Technology (COBIT

Figure 15—The COBIT Cube



Delivered by

Professional Services

Managed Services

Hardware & Software

Source: IT Governance Institute, Control Objectives for Information and related Technology (COBIT) 4.0.

Security Framework

- SECURITY COMPLIANCE
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- IDENTITY & ACCESS
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- DATA SECURITY
  - Protect and secure your data and information assets
- APPLICATION SECURITY
  - Continuously manage, monitor and audit application security
- INFRASTRUCTURE SECURITY
  - Comprehensive threat and vulnerability management across networks, servers and end-points

PEOPLE AND IDENTITY

Manage Identities and Access

"How can my business benefit from management of digital identity?"

Issues

- Understanding the identity risk gap
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Dormant IDs or shared identities being used to inappropriately access resources
- Failing an audit

Security Solution

- ***Identity Lifecycle Management:***
- ***High-Assurance Digital Identities:***
- ***Identity Audit***

Values

- Reduces the cost, increases efficiency and enables audit-ability of managing flow of users entering, using, and leaving the organization
- Decreases risk of internal fraud, data leak, or operational outage
- Supports globalization of operations
- Enables shift from traditional brick & mortar sales to delivery of on-line services to customers and partners across the globe
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on

Data


Security Framework
Security Governance, Risk Management and Compliance
People and Identity
Data and Information
Application and Process
Network, Server, and End-point
Physical Infrastructure
Common Policy, Event Handling and Reporting

DATA AND INFORMATION

Protect Data and Information

"How can I reduce the cost and pain associated with tracking and controlling who touched what data when? How do I assure that my data is available to the business, today and tomorrow?"

Issues

- Data stored on removable media that can be lost/stolen
- Data stored in the clear is easily accessible
- Inconsistent data policies
- Unstructured data
- Legal, regulatory and ethical exposure for the organization
- Costs of data breaches, notification, brand value
- Failing an audit

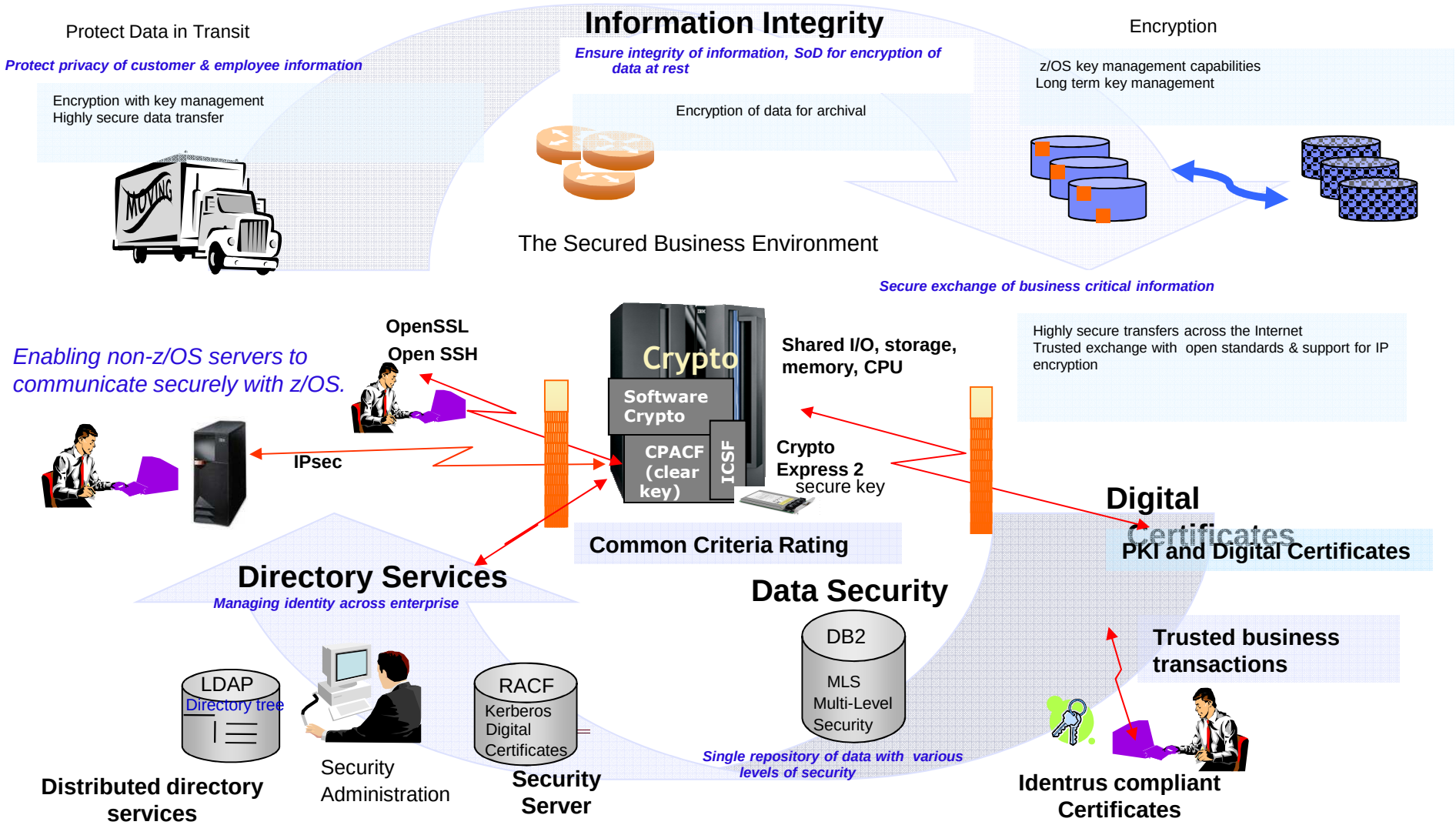
Security solution

- ***Data Classification*:**
- ***Data Encryption*:**
- ***Data Masking*:**

Values

- Reduces the cost, increases ability to meet audit and compliance mandates
- Provides a cost-effective way to meet legal discovery, hold and retention requirements
- Assures data is available to the right people, at the right time
- Assures data is not deliberately or inadvertently taken, leaked, or damaged
- Decreases number and complexity of controls integrated within the enterprise

Cryptography

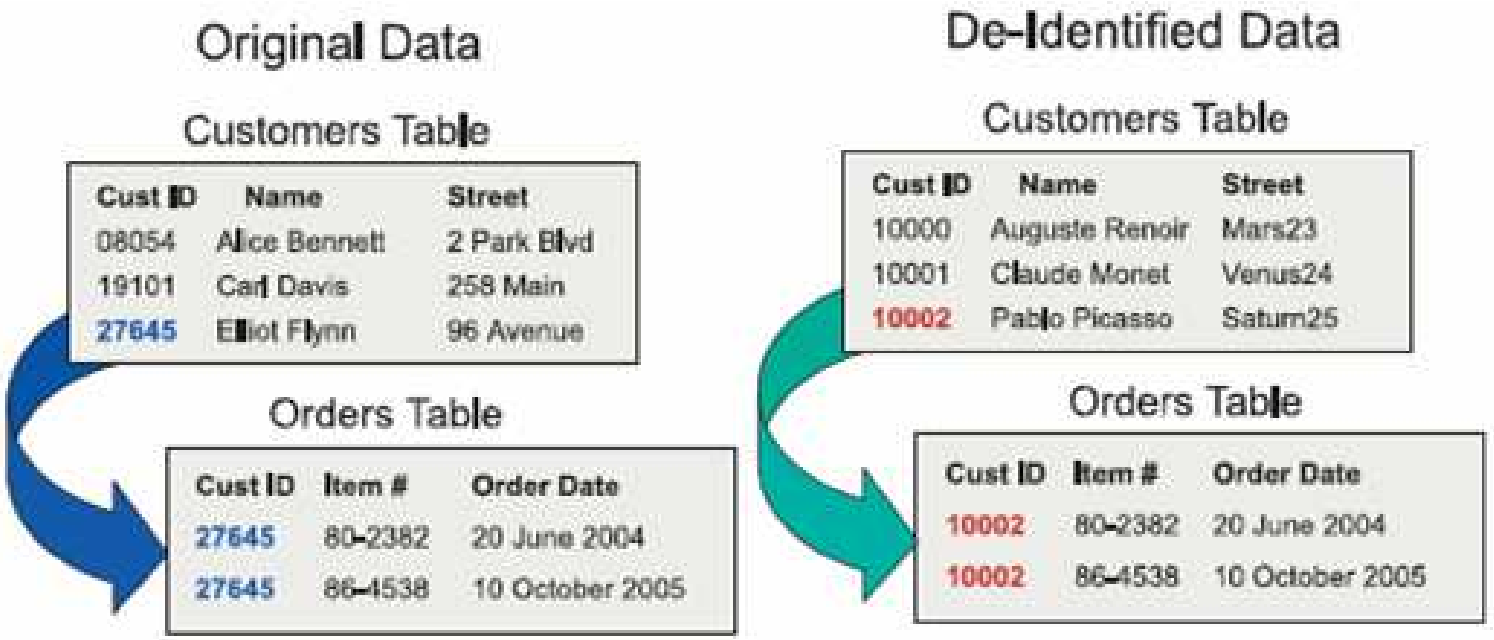


Key Management and Key Serving

Key management components

- Key store – choice of using existing key store or installing new hardware implementations or software only
- Key serving – transparent detection of media and assignment of keys
- Key management – backup and synchronization, life cycle, audit, and long term retention

Test and Dev versions of Prod DB's



Optim offers a variety of data masking techniques to protect the confidentiality of private information.

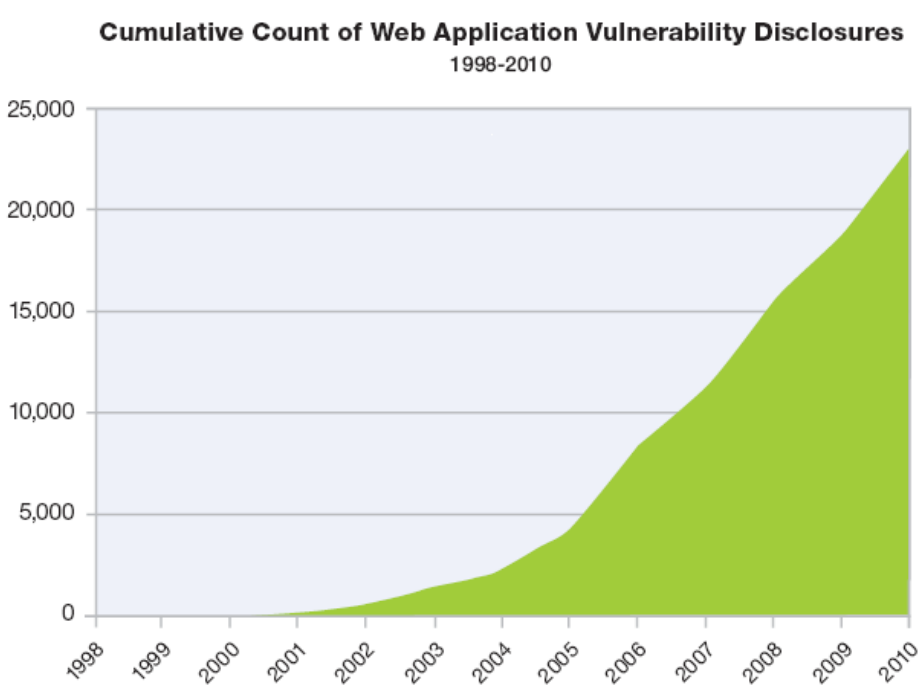
Production → Test/Dev

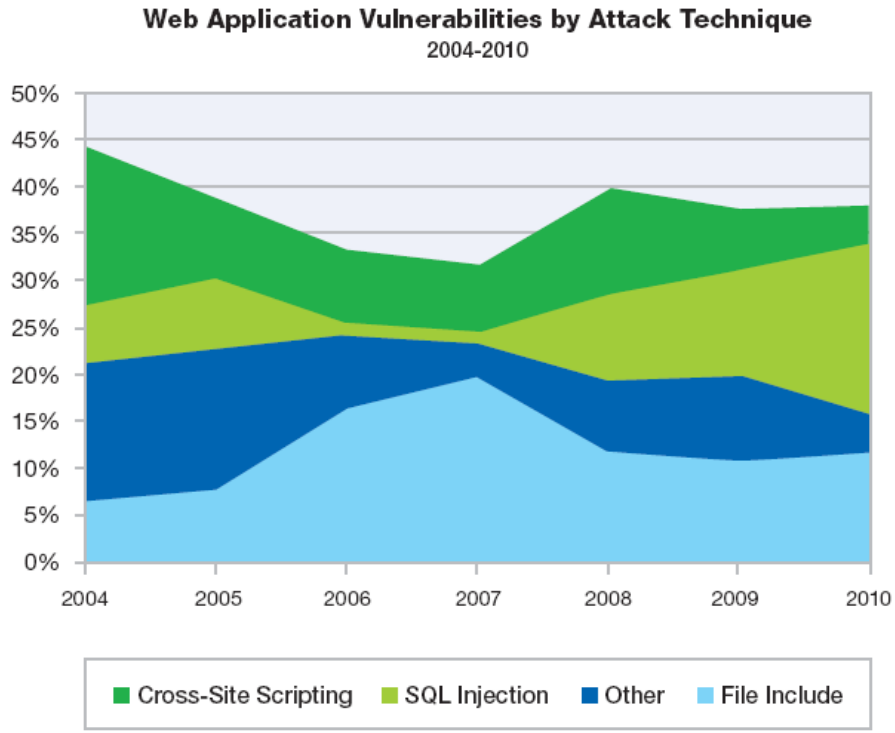
Application

Application Vulnerabilities Continue to Grow

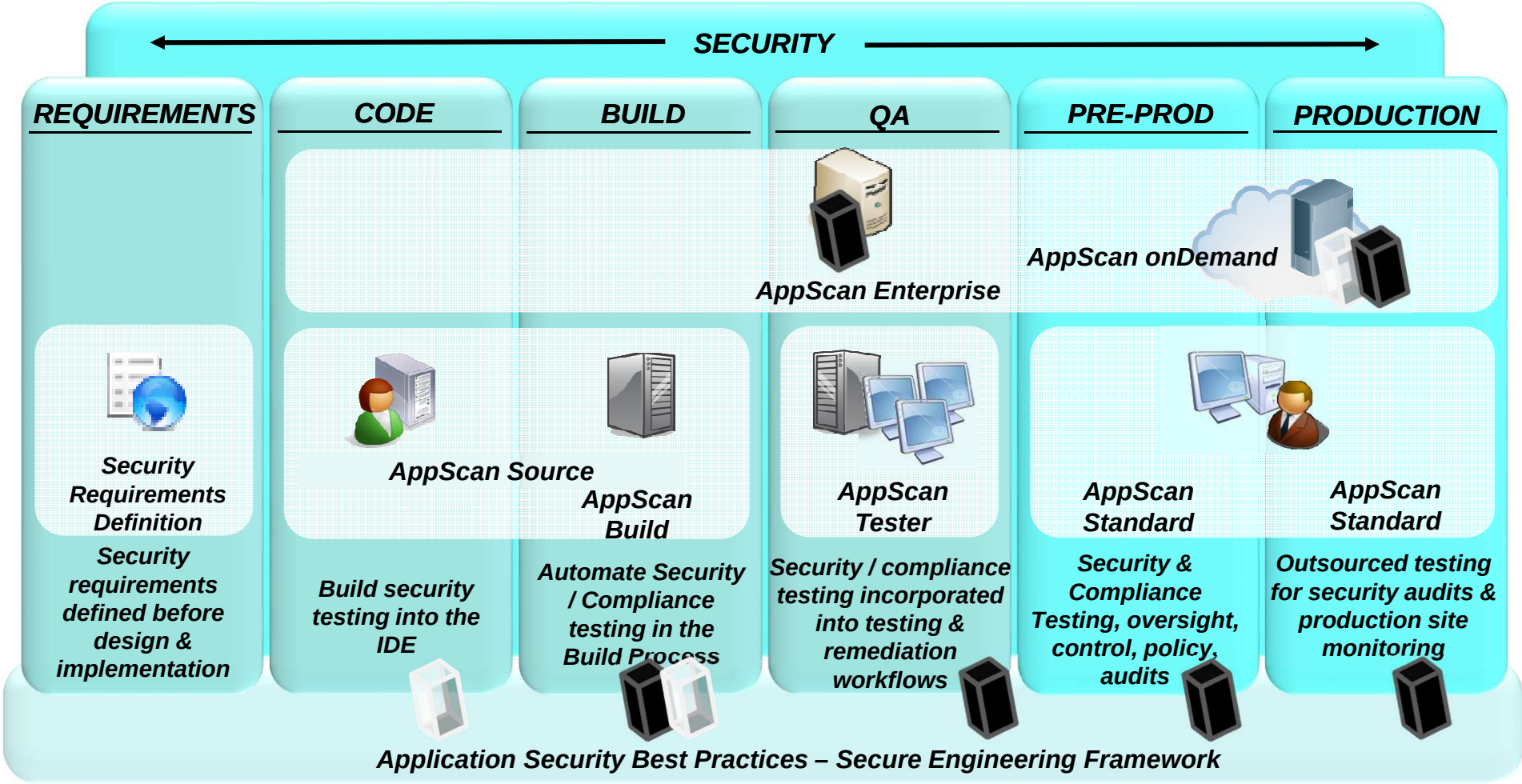
Web application vulnerabilities dominate enterprise threat landscape

- **49%** of all vulnerabilities are in web applications*
- Cross-Site Scripting & SQL injection vulnerabilities continue to dominate





Application Vulnerability Management



Dynamic Analysis/Black box –

Static Analysis/White box –

Execute what you trust !!!

Code signing for Program loading or execution

Network server …

NETWORK, SERVER AND END POINT

Manage Infrastructure Security

"How does my business benefit from infrastructure security protection?"

Issues

- Mass commercialization and automation of threats
- Parasitic, stealthier, more damaging attacks
- Poor understanding of risks in new technologies and applications, including virtualization and cloud
- Weak application controls
- Lack of skills to monitor and manage security inputs
- Compounding cost of managing an ever increasing array of security technologies
- Undetected breaches due to privilege access misuse and downtime from incidents
- Inability to establish forensic evidence or demonstrate compliance

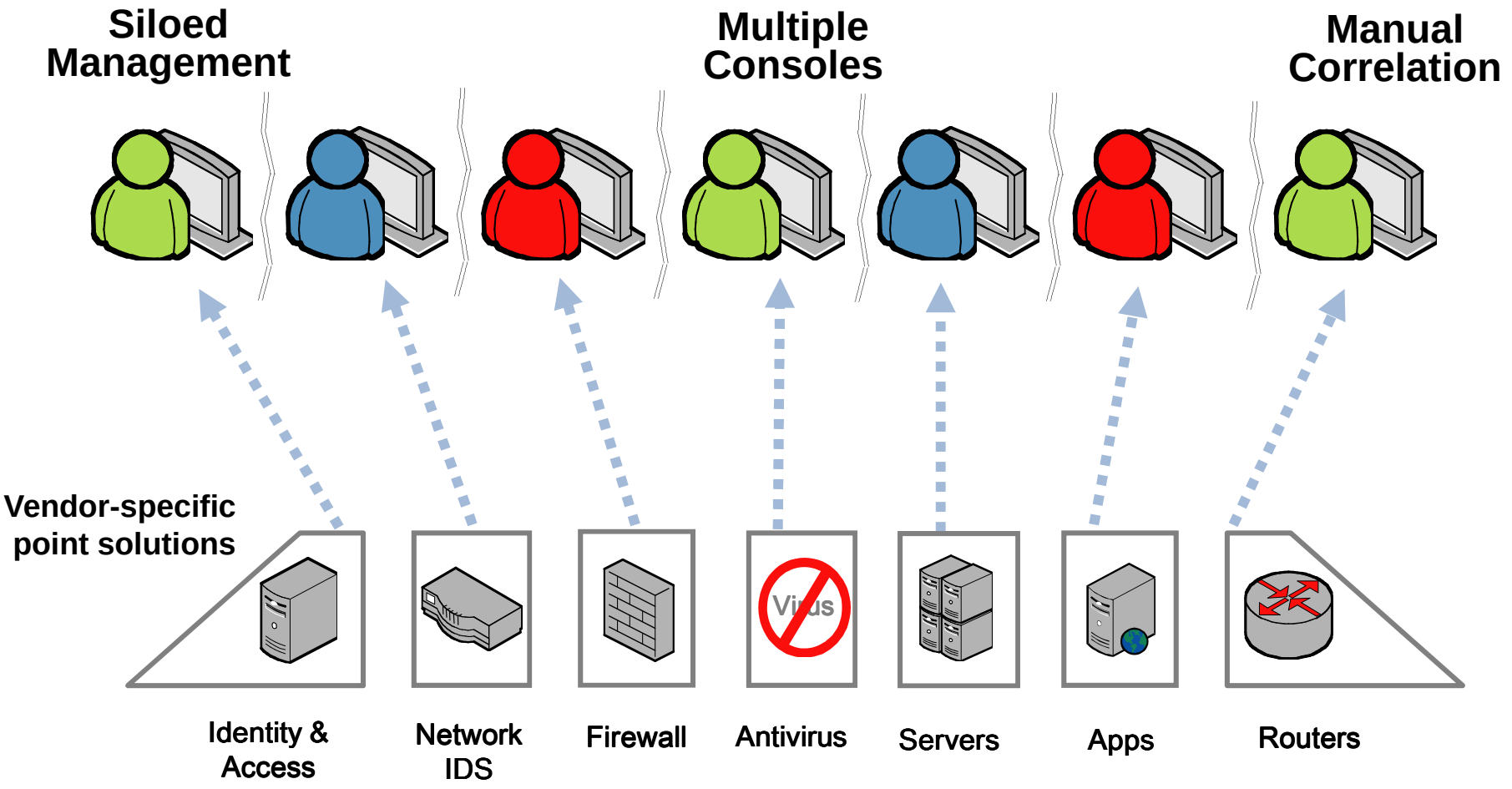
Security Solutions

- ***Network Threat Mitigation***: Network and Endpoint Intrusion Detection and Prevention
- ***Disk tape*** :encryption
- ***Server Security*** : hardware cryptography

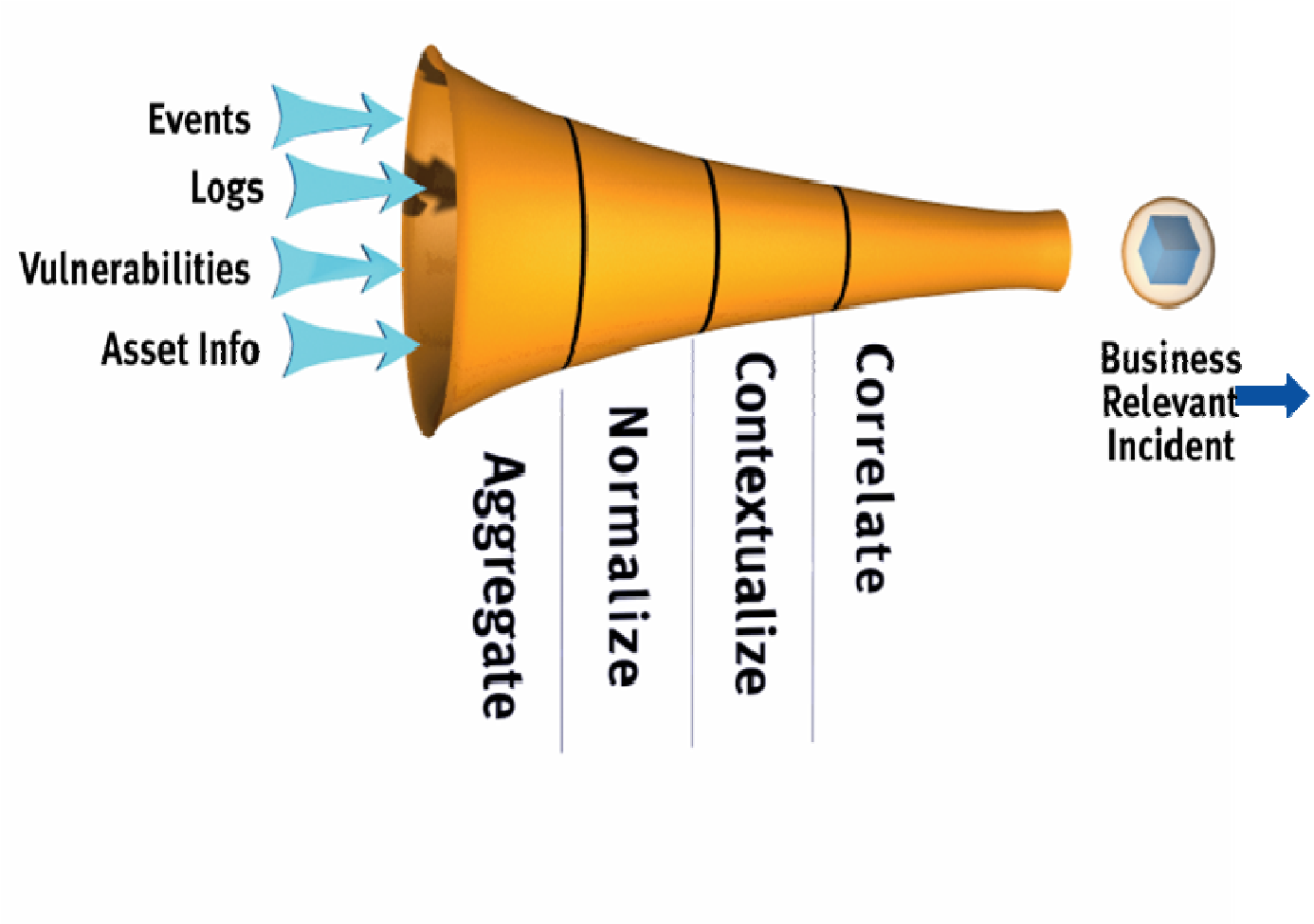
Values

- Reduces cost of ongoing management of security operations
- Improves operational availability and assures performance against SLA, backed by industry's only guaranteed SLA for managed protection services
- Increases productivity by decreasing risk of virus, worm and malcode infestation
- Decreases volume of incoming spam
- Drill down on specific violations to quickly address resolution
- Readily show status against major regulations

SOC = Security Operation Center



In house – Collect, Correlation, Relevance !



HSM is an increasingly important Quality of Service differentiator for IBM and for the competition

- **Definition**

  – A **Hardware Security Module** (often abbreviated to **HSM**) is a physical device in form of a plug-in card or an external security device that can be attached to general purpose computer and servers.

  – HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. The cryptographic material handled by most HSMs are asymmetric key pairs (and certificates) used in public-key cryptography.

  – Some HSMs can also handle symmetric keys and other arbitrary data. Many HSM systems have means to securely backup the keys they handle either in a wrapped form via the computer's operating system or externally using a smartcard or some other security token. HSMs should never allow for secrets exportation in plaintext form, even when migrating between HSMs or performing backup operations.

- **…very compete market**

AEP	Bull	SafeNet	Thales eSecurity	…
ASI	Futurex	PRISM	True Access	
ARX	HP	Smart Card Technology Inc	Utimaco	
Banksys	REALSEC	Sun	xyzmo	

HSM – Different flavors

Appliances - *Network level*

+ Easy to set in place
+ Small Scalability (Stacking)
+ Network Functionalities
+ Clear Key / Secure Key
+ Safe Key Repository
+ Easy to install/remove

- **Network Architecture dependant**
- Wires, Software management complexity
- Network Bandwidth management overhead
- Energy consumption
- Requires large stack of API for multiple workload purposes
- Can't be virtualized

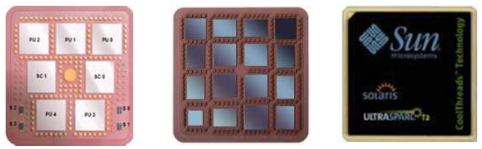
PCI-X, PCI-E - *Machine Internal Level*

IBM

+ Easy to put in place
+ Medium Scalability
+ Internal Architecture Functionalities
+ Clear Key / Secure Key
+ Safe Key Repository

- **Internal PCI-E Bandwidth**
- Dependant on the number of PCI-X,PCI-E ports
- Virtualization of the resources to be proven for each platform/environment
- Requires large stack of API for multiple workload purposes

On the silicon – *Processor Architecture Level*

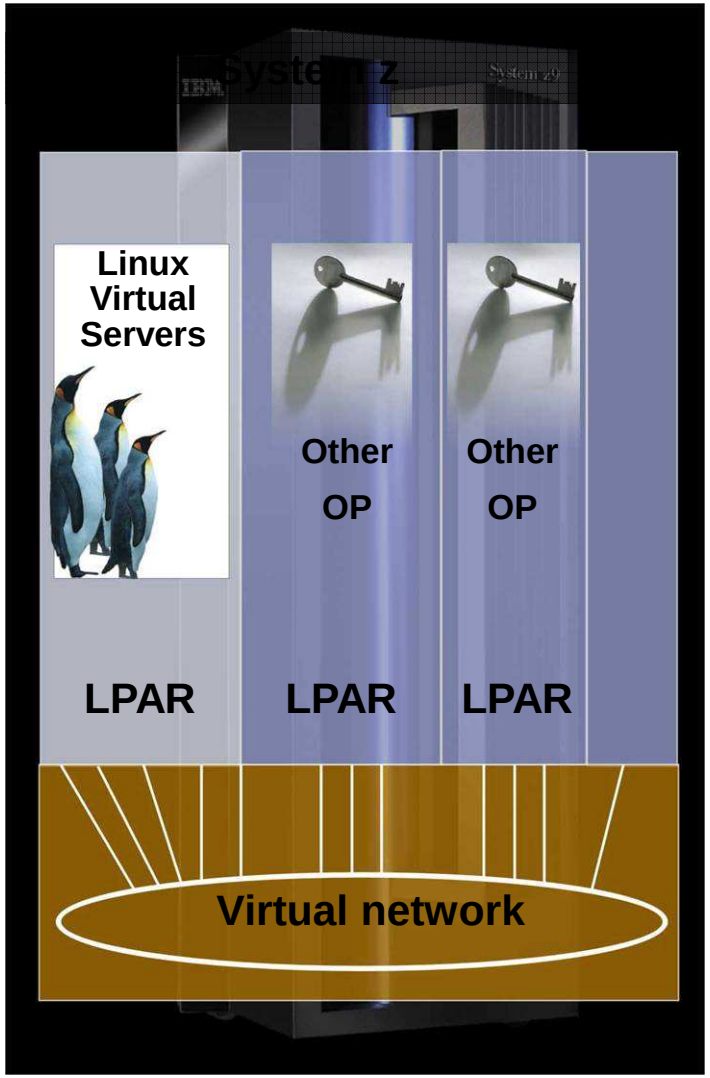


IBM IBM

+ Performance / Throughput
+ High Scalability
+ Features already onboard
+ Ease of use
+ Virtualization
+ Energy Efficiency
+ Clear Key / Protected Key (GA3)

- Limited Set of Supported Algorithms
- Evolution is linked to the Processor architecture
- Crypto workload is consuming the same CPU cycle as multi-purpose workload
- Requires large stack of API for multiple purposes

Security through virtual infrastructure ???



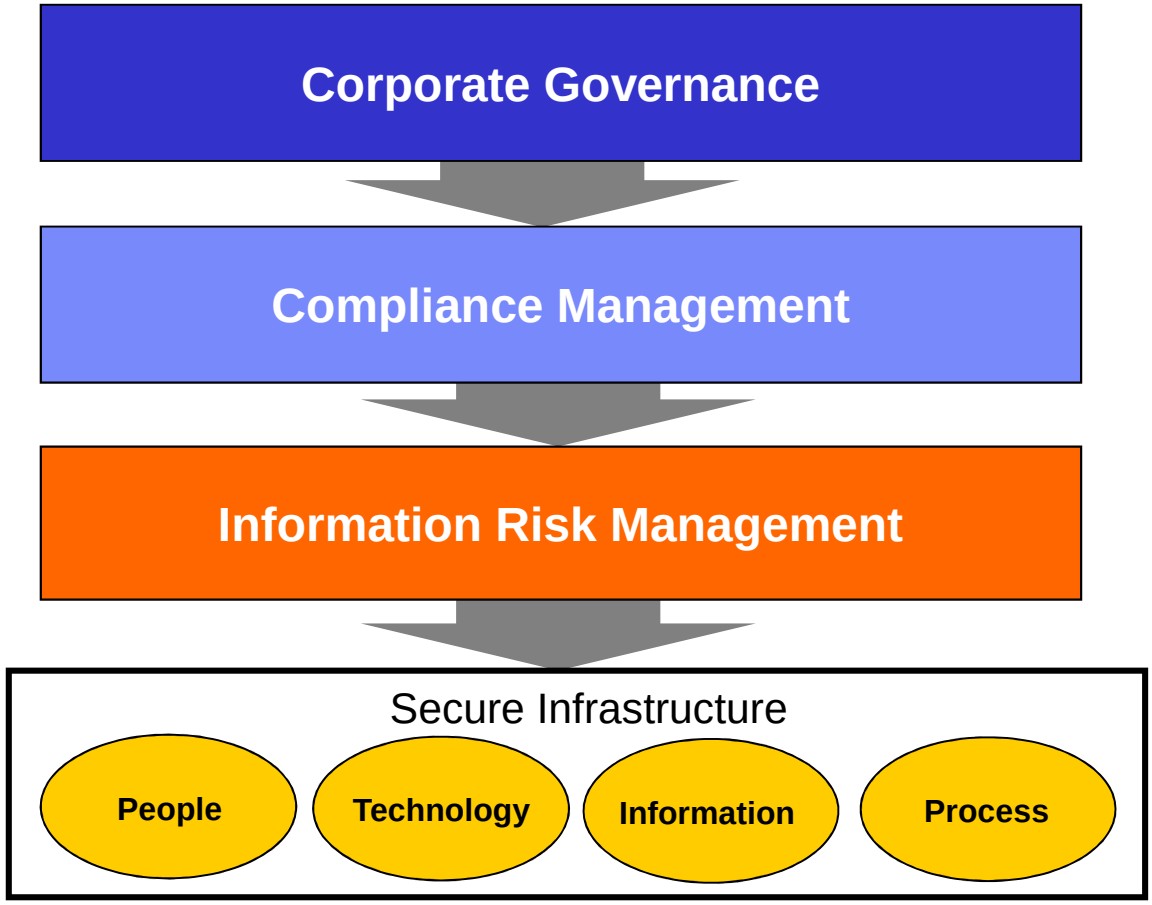
- Virtual servers
- Virtual network
- Virtual disk

SECURITY COMPLIANCE

- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

What is a comprehensive strategy ?

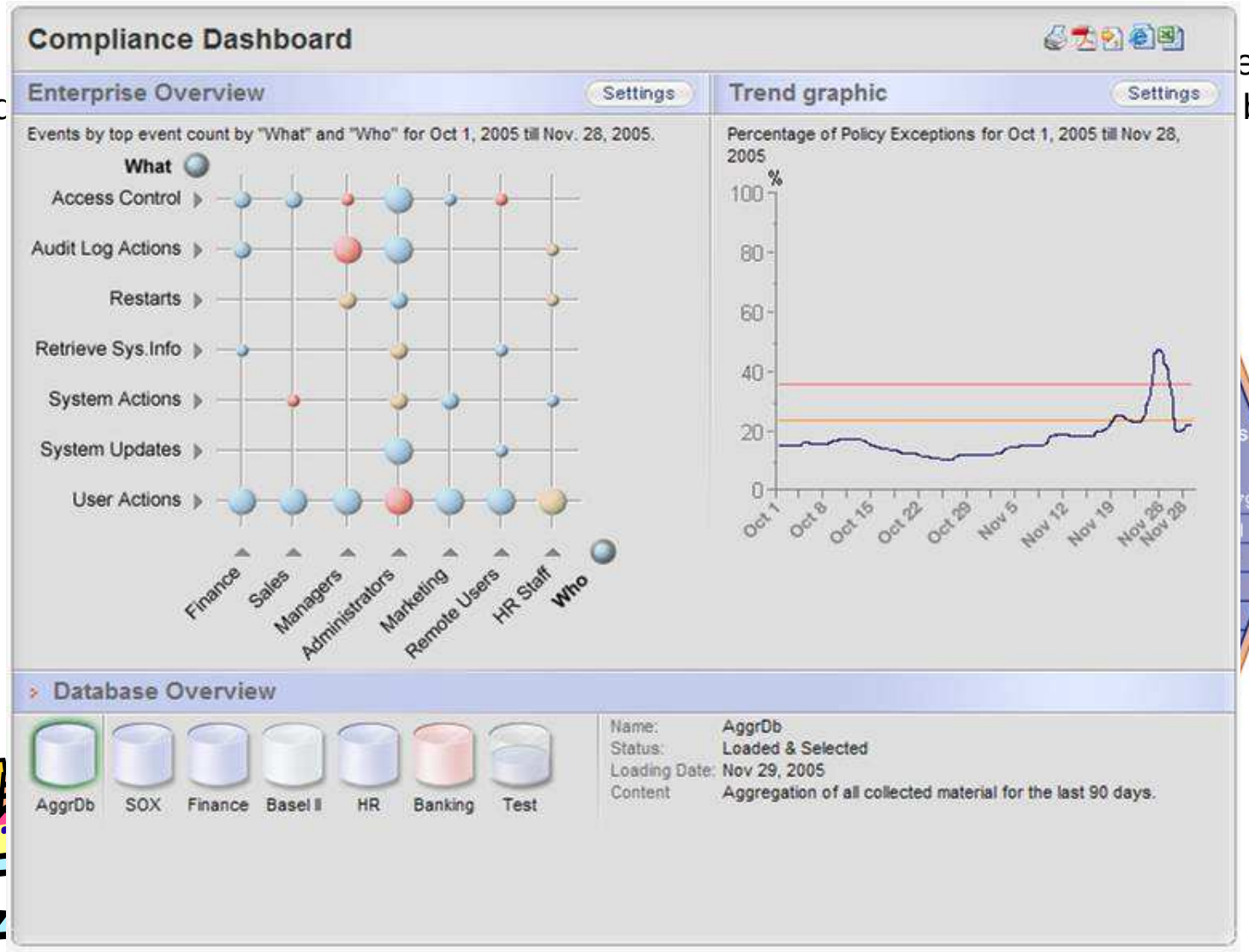
Governance



"Every time we do technology first, it has been a failure. Security strategy must be driven by core business processes."

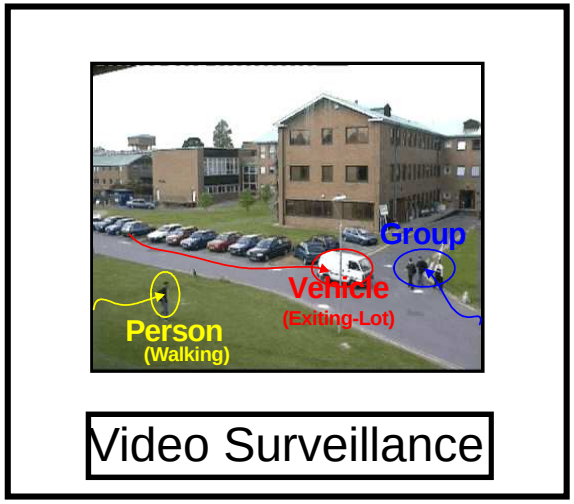
– CISO, Fortune 100 Bank

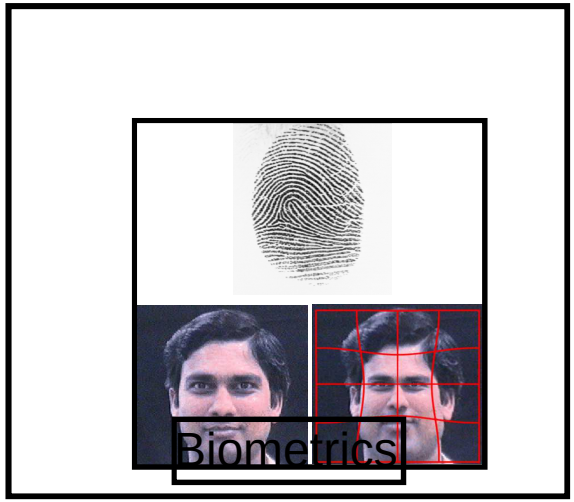
Compliance monitoring

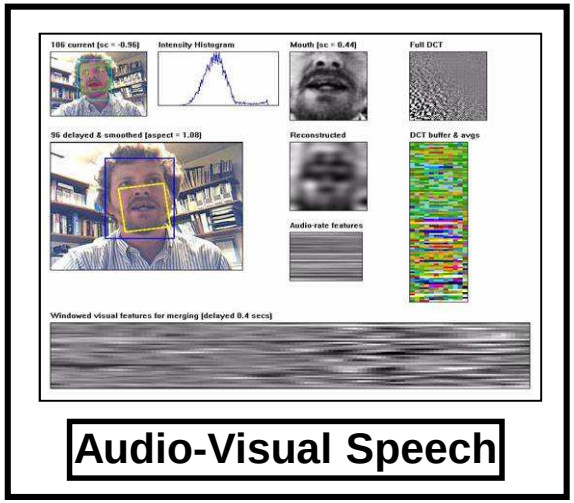


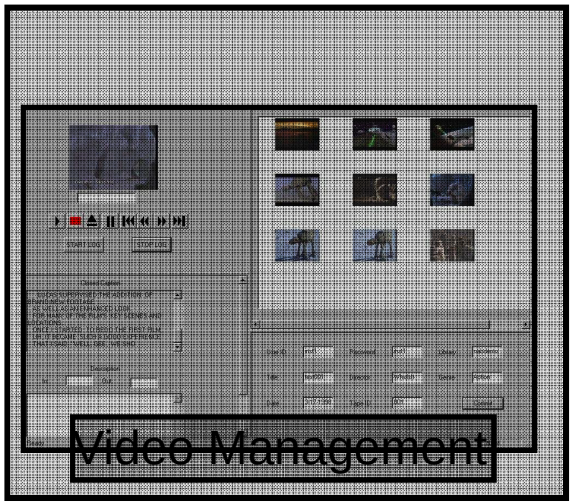
Physical infrastructure

Physical security Computer Vision Projects

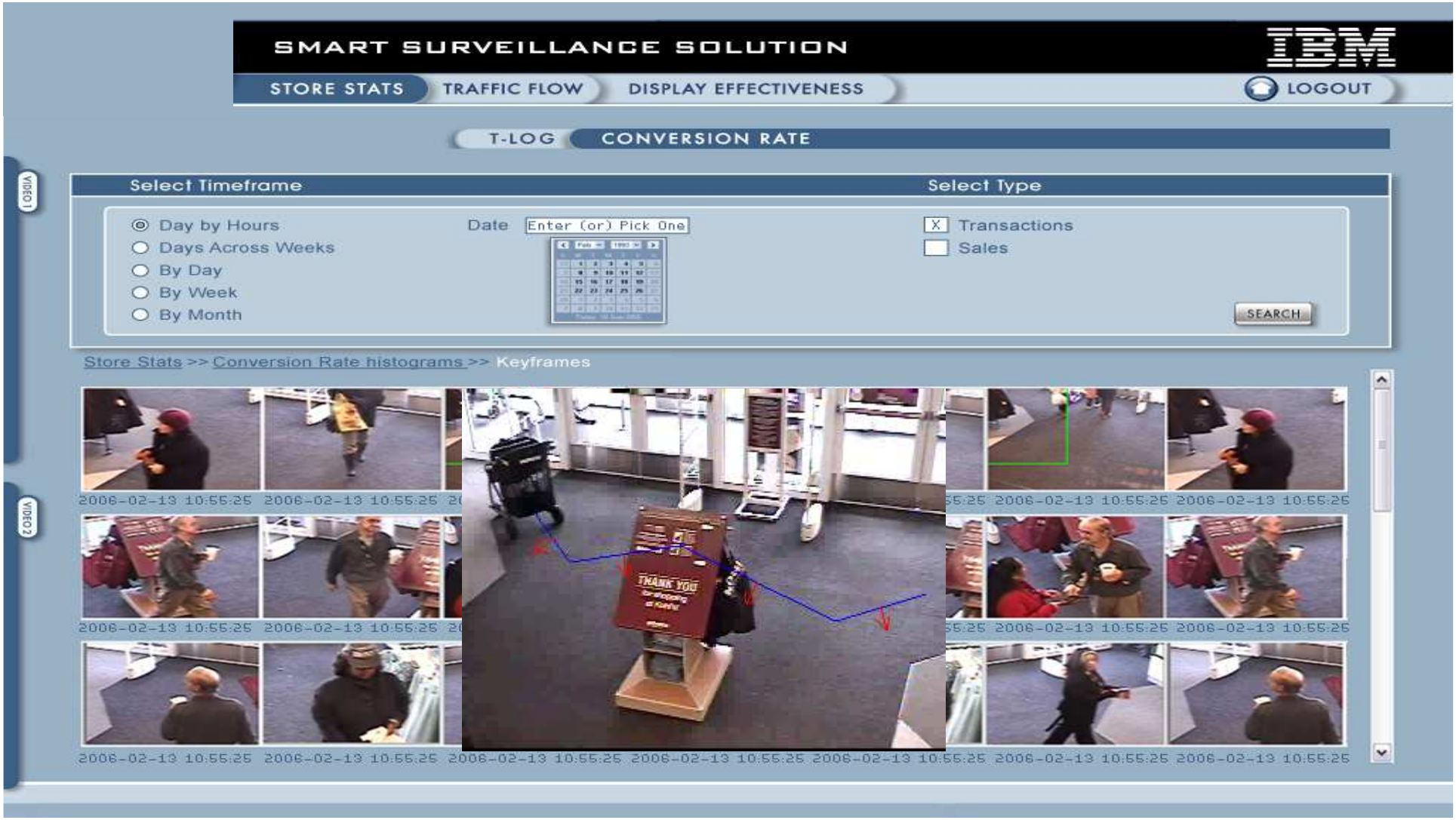




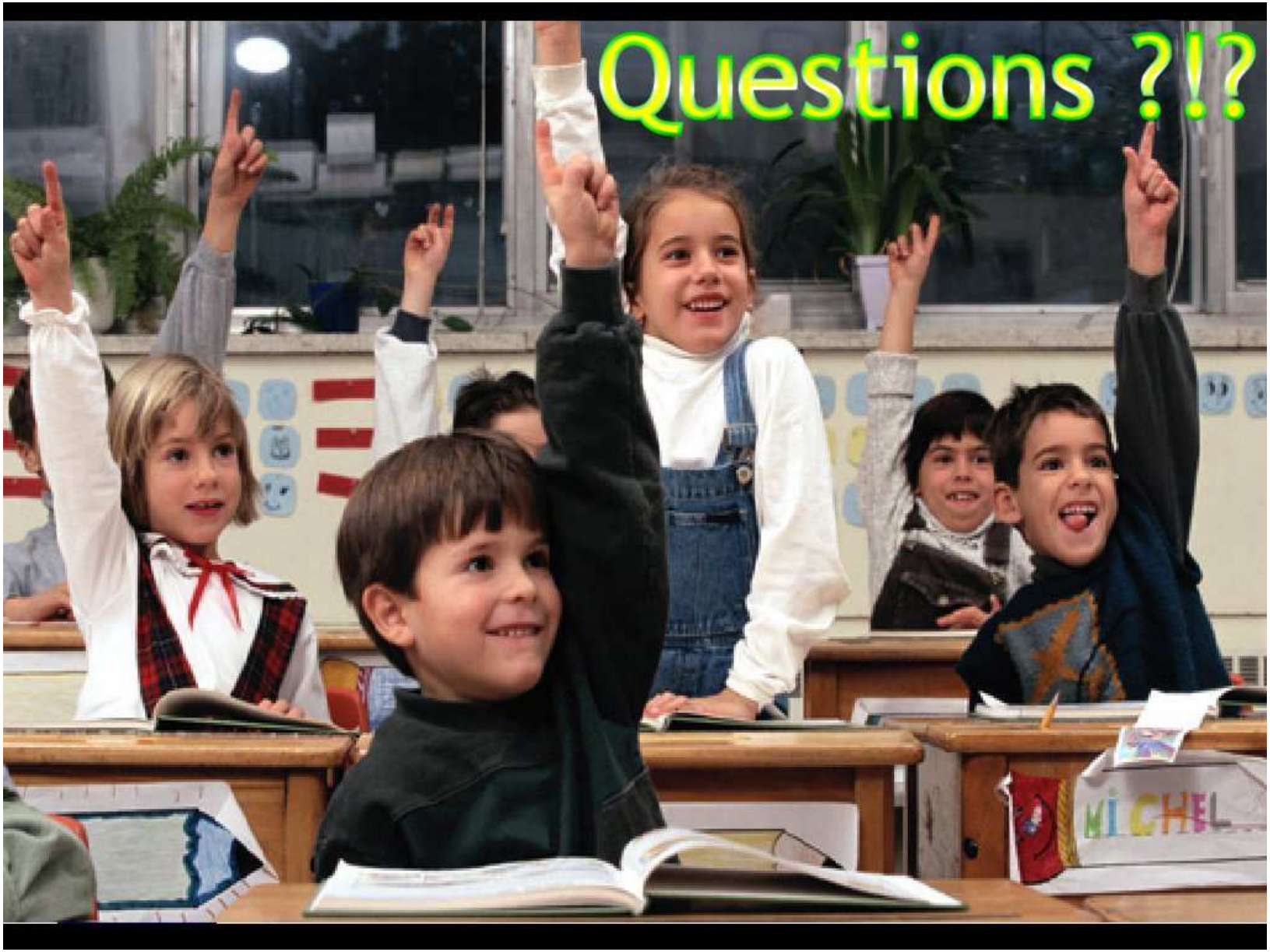




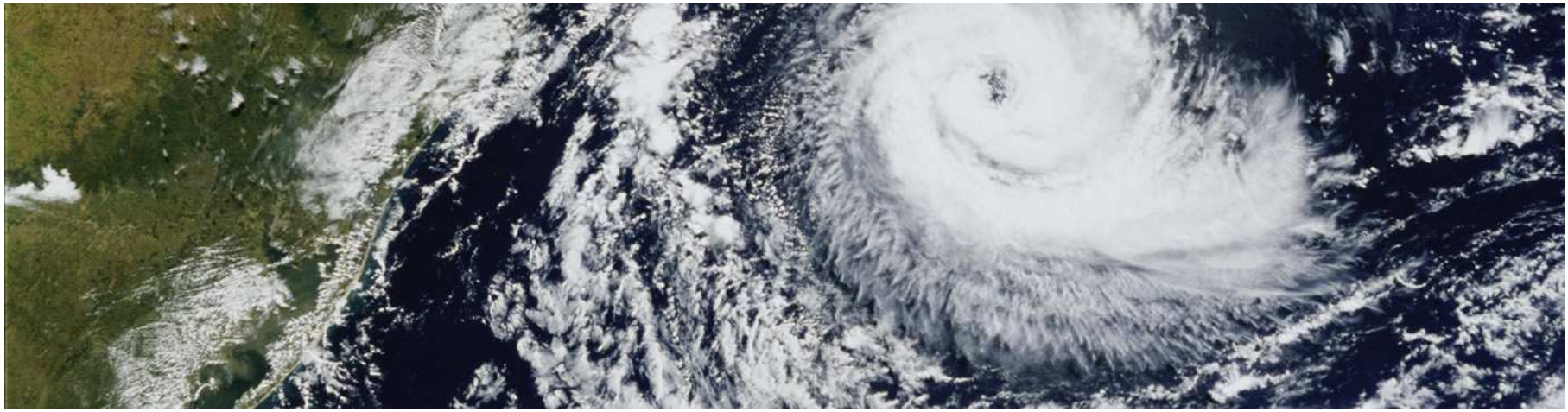
People counting - people capture and recognition



Returns fraud - people capture and recognition


Questions ?!?

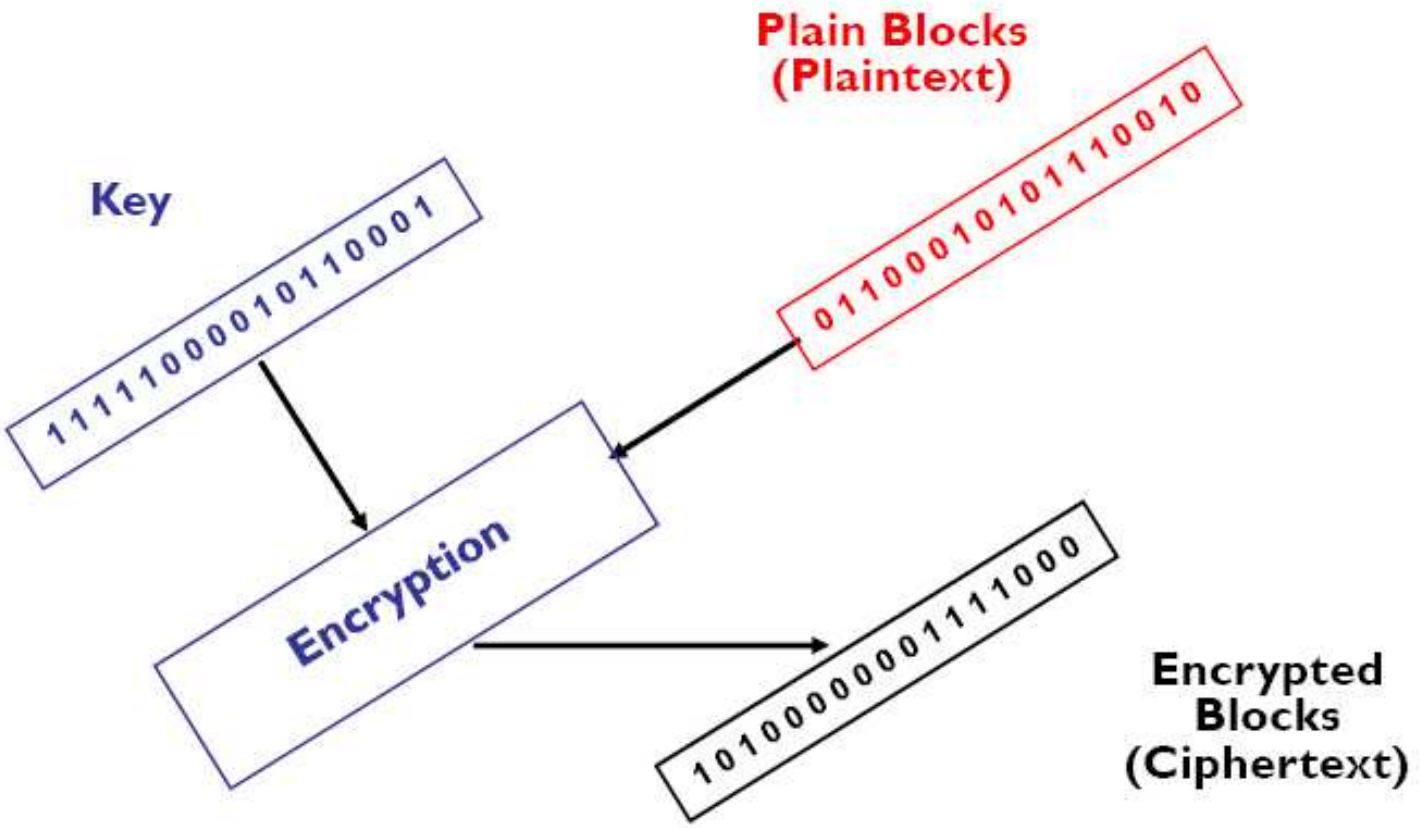
La Cryptographie clé de la sécurité technologique



Encryption begins

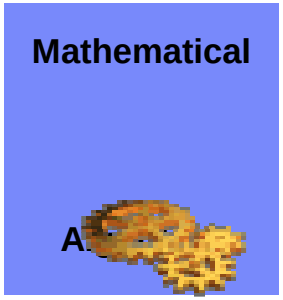
- **Coming from military and diplomatic for “secret writing” activities**
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - DEFGHIJKLMNOPQRSTUVWXYZABC
  - Replace the letter in top line by the one underneath (substitution)
  - Reverse the order of the letters in the message (transposition)
  - The above scheme is known as the Caesar Cipher
  - Reputed 1st used by Julius Caesar during the Gallic wars
- **Cryptography (Greek “cryptos" (hidden) + "graphia“ (writing))**

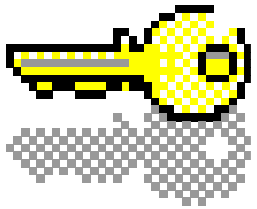
Secret key Public algorithm



Cryptographic System Components

In mathematics, computing, linguistics, and related disciplines, an **algorithm** is a procedure (a finite set of well-defined instructions) for accomplishing some task which, given an initial state, will terminate in a defined end-state.

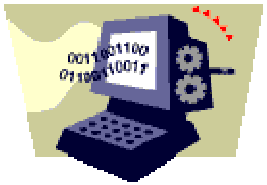


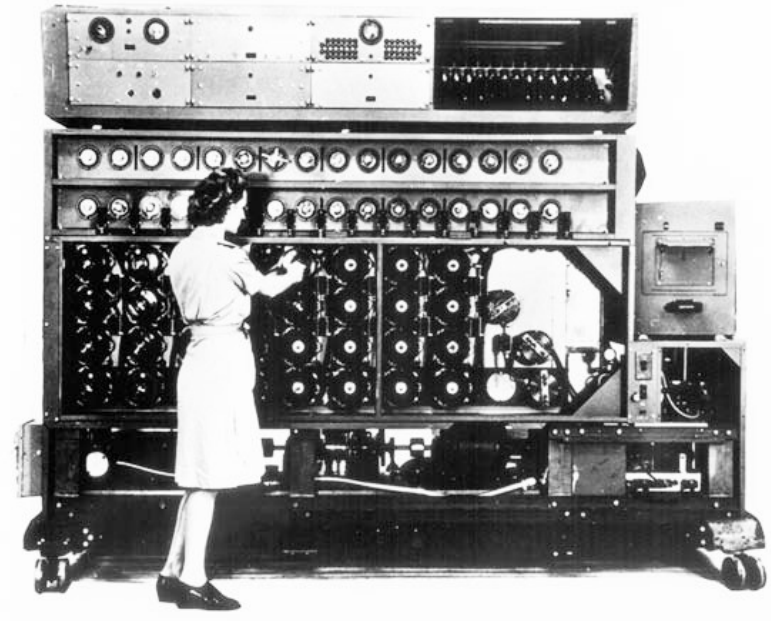


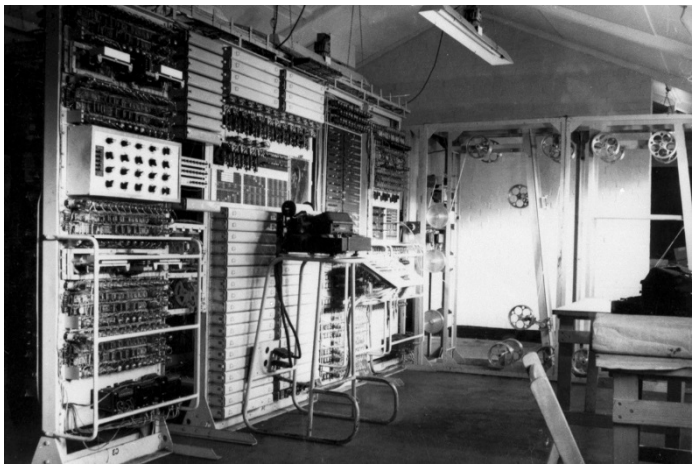
Cryptographic Key

The algorithms are publicly known. A **cryptographic key** is a piece of information that controls the operation of a cryptography algorithm. The keys are responsible for keeping the algorithm execution secret.

Begin of IT







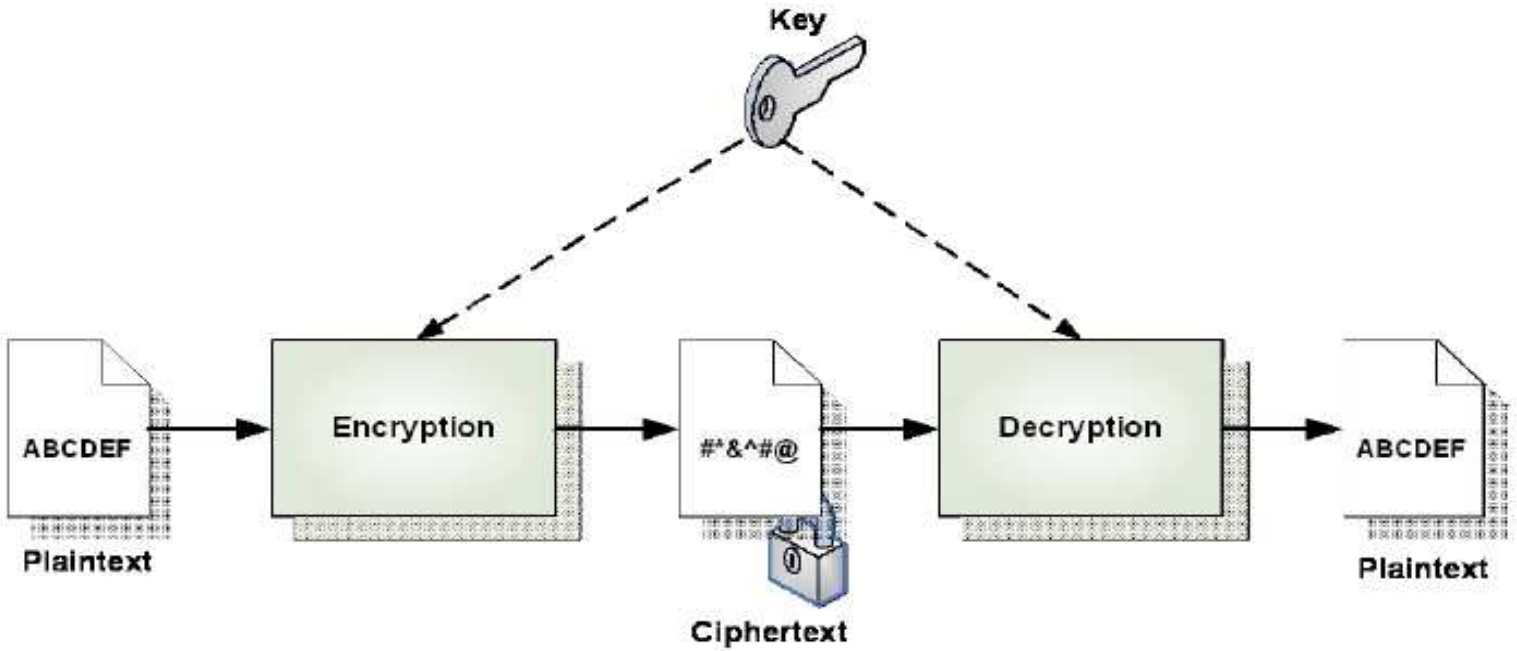
Three Major Types of Encryption

- Symmetric Keys
- Asymmetric Keys
- Hash

Systems May Use Both

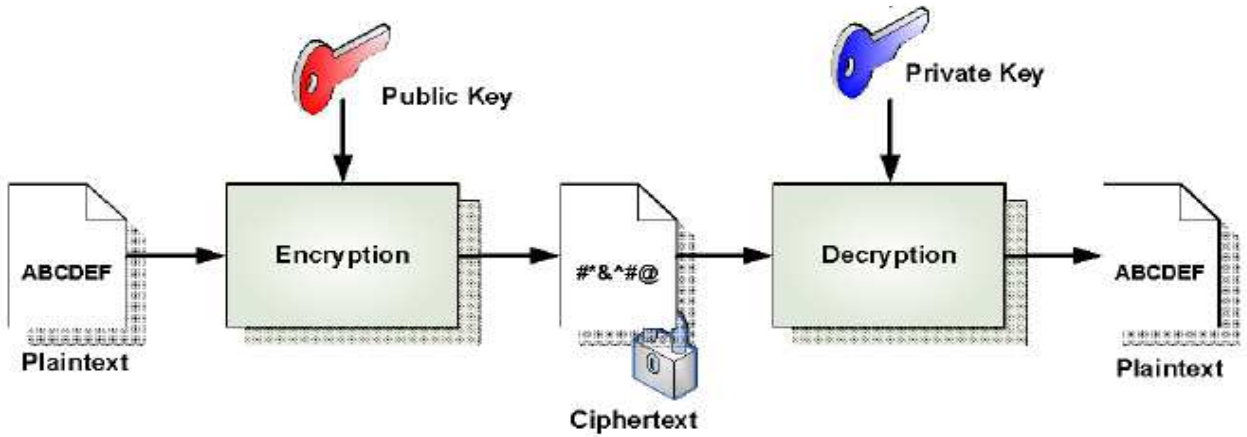
Symmetric Key

- One Key
- Used for Both Encryption and Decryption
- Requires Lower Computing Power



Asymmetric Key

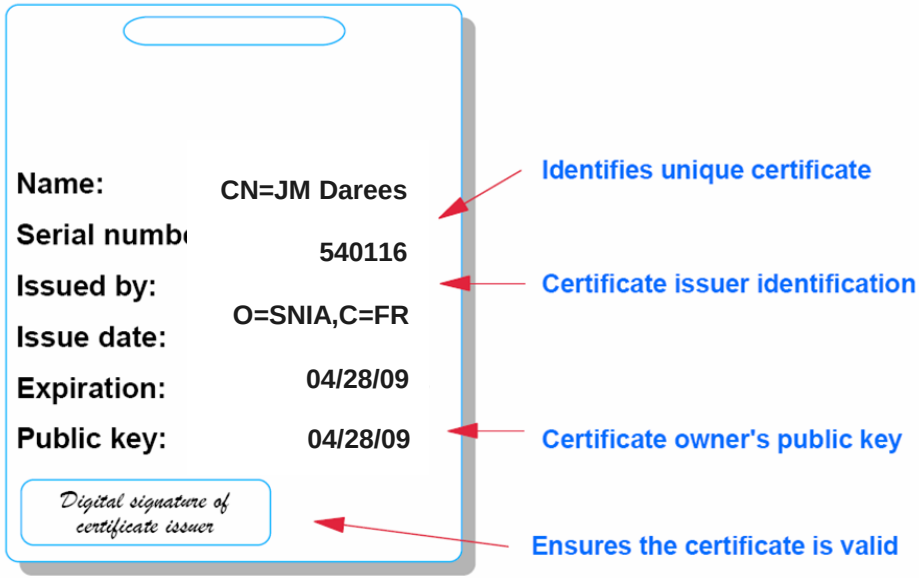
- Uses Private and Public Key Pair
  - Can't be Derived from Each Other
  - Data Encrypted with One Can Only Be Decrypted With the Other



Certificates

- Digital document that give evidence that a public key's belongs to whom it may concern. It contains at least the information listed below:
  - Public Key
  - Certificate owner's Identity
  - Expiration Date
  - Signature from a third part
  - An utilization

- Sample of use:
  - Tax Declarations Online
  - Secure Internet
  - Internet Authentication Mechanisms



Hashing

- Hashing does not encrypt data, but provides transformation used to verify data integrity
  - Hash algorithm digests data and represents its bits and bit patterns by fixed-size equivalent - a Hash Value
    - Size of the value is fixed by the algorithm (SHA-1 is 20 bytes)
    - Algorithm is non-reversible: cannot reproduce data from hash
    - Single bit change in data may change half of the bits in hash
- Hash also used as “digital signature”

Pay US$ 100 to JM Darees =
5064c498576ec57e9e75fbb04ee8ccaa58c29c1a

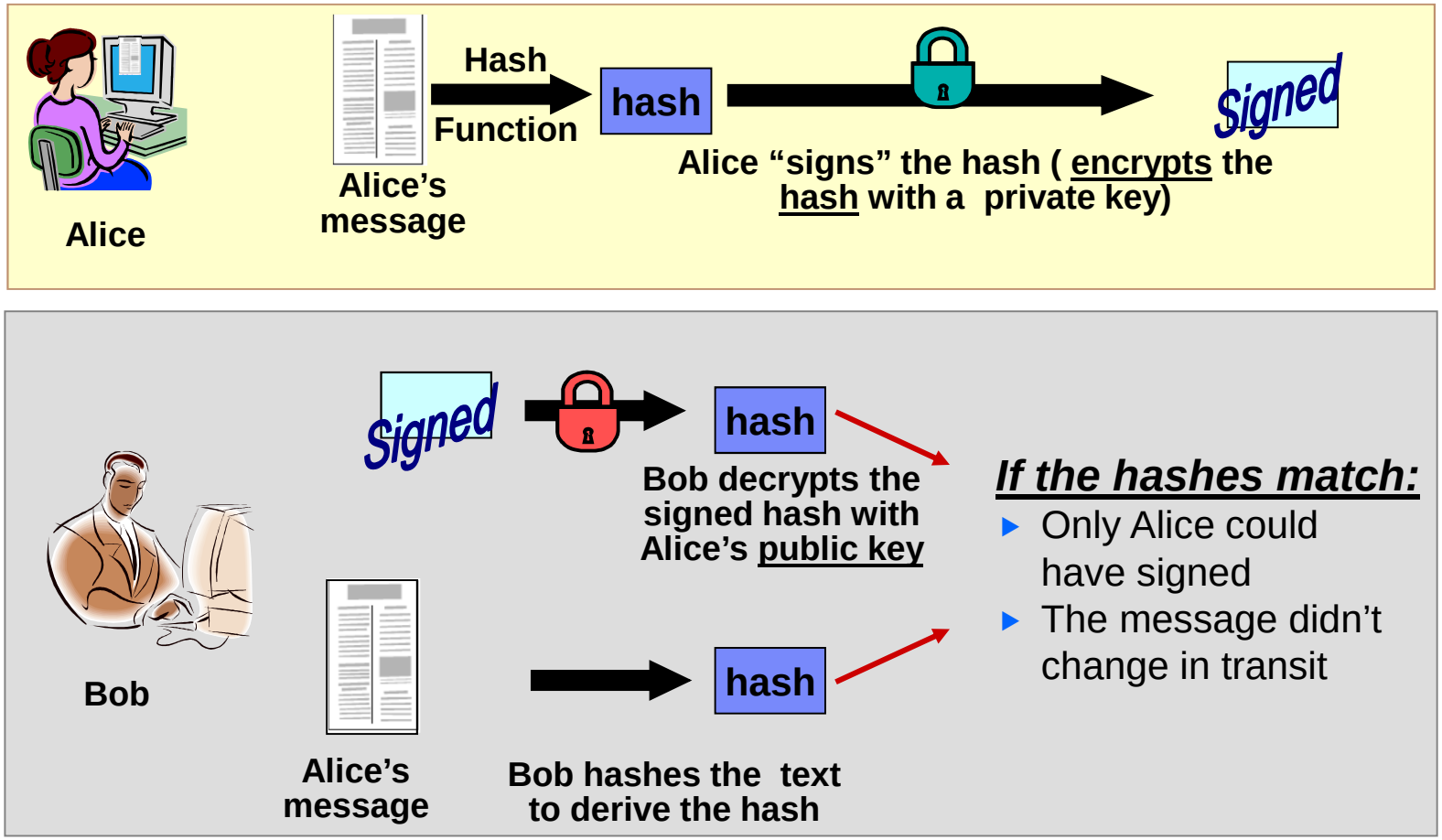
Pay US$ 100 to JM Dares =
83a8e63994fba9d9c927dd6fcf7c92ddc3185063

SSL combines symmetric and Asymmetric

- **Handshake – Asymmetric**
  - Signature Verification
  - Public Key
- **Record Level – Symmetric**
  - DES/TDES
  - AES
  - Hash

How do Digital Signatures Work?

All major digital signature signing techniques involve first hashing the data then signing the hash.



Bob can be sure that the message came from Alice!

Cryptographic Algorithms And Their Use

	Symmetric SYM	Asymmetric ASYM	Hash HASH	Digital Signature ASYM HASH	SESSION SYM *(Session Key)* ASYM HASH
					
Confidentiality	X				X
Integrity			X	X	X
Authentication		X		X	X
Non-Repudiation		X		X	X

Key algorithms

- ***DES***
- ***T-DES***
- ***AES***
- ***RSA***
- ***DSA***
- ***MD5***
- ***MAC***
- ***MDC***
- ***SHA***

The Key Management Problem

Many Key Uses

- Private signature key
- Public signature verification key
- Symmetric authentication key
- Private authentication key
- Public authentication key
- Symmetric data encryption key
- Symmetric key wrapping key
- Symmetric and asymmetric random number generation keys
- Private key transport key
- Public Key Transport Key
- Symmetric Key Agreement Key
- Private Static Key Agreement Key
- Public Static Key Agreement Key
- Private Ephemeral Key Agreement Key
- Public Ephemeral Key Agreement Key
- Symmetric Authorization Key
- Private Authorization Key
- Public Authorization Key

Key Management VS Time

- **Key and Data Lifetime**
  - Forever
    - Assure Access to Data Years from Now
  - For a Limited Time Period
    - Ephemeral – Milliseconds, Seconds
    - Weeks, Months, Years
- **What Happens at End of Life?**
  - Mandatory Re-Encryption
  - Destruction of Data
  - Destruction of Key

Key Management Process

- **Policies**
  - Who Can Establish Keys?
  - Who Can Delete Keys?
  - What is the Lifetime of a Key?
  - Can the Key be Archived?
  - Are the Keys Changed Periodically?
  - Are Keys Automatically Deleted or Archived?
  - Who Else Can Use the Key?

- **Auditing**
  - Track the Key over it's Lifetime
  - Who Created the Key and When?
  - Who Changed the Key and When?
  - Who Created a Copy of the Key and When?
  - Where are the Copies of the Key
  - Who Deleted the Key and When?

Why we need key management

- Regulatory Compliance
  - PCI-DSS (PCI – Data Security Standard)
  - PCI PIN Security Requirements
  - Digital signature requirements in the public sector
- To be secure ... ultimately the security depends directly on:
  - the key material – randomness
  - the effectiveness of mechanisms and protocol – algorithm
  - and the protection afforded to protect the keys – key management

PCI-DSS Key Management Requirements (3.5 and 3.6)

- Protect any keys used to secure cardholder data against disclosure and misuse - also key encrypting keys.
- Restrict access to cryptographic keys to the fewest number of custodians necessary.
- Fully document and implement all key-management processes and procedures for cryptographic keys.
- Cryptographic key changes for keys that have reached the end of their crypto period (key rotation)
- Store cryptographic keys securely in the fewest possible locations and forms
- Secure cryptographic key storage
- Split knowledge and establishment of dual control of cryptographic keys

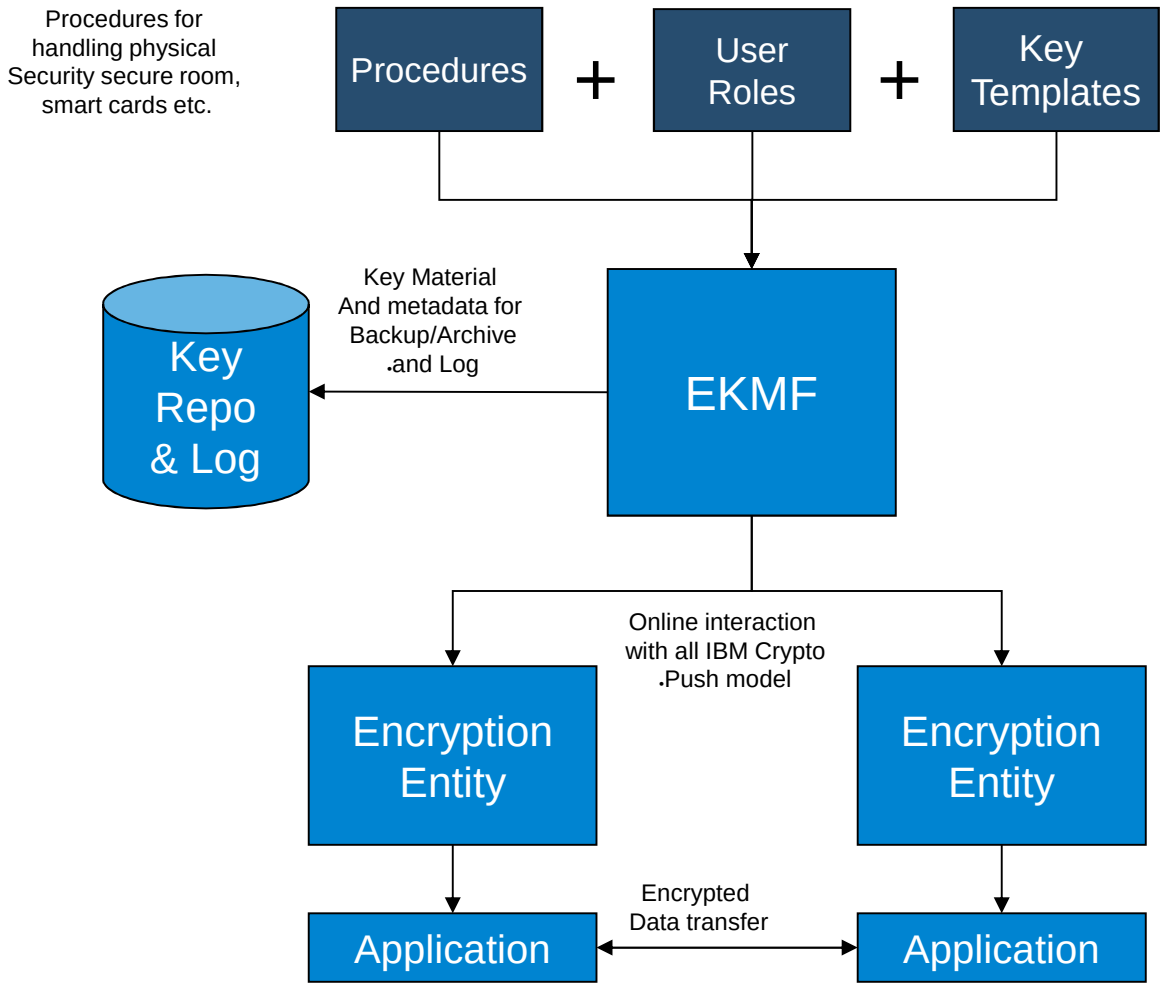
PCI PIN Security Requirements

- Formerly known as VISA and MasterCard PIN Security Requirements
  - Requirements for securing PINs and encryption keys and PIN-based transactions.
  - Effective from September 2011
- Summary of key management requirements:
  - Compromise of key generation not possible without collusion between two trusted individuals
  - Tamper responsive cryptographic hardware
  - Dual control for access to HSM environments
  - Separation of duties
  - Split knowledge for handling clear key components
  - Audit trails for all key management operations
  - Key changes in accordance with recommended crypto periods (ie. NIST SP800-57)
  - Document all key management processes

Summary of Key Management Requirements

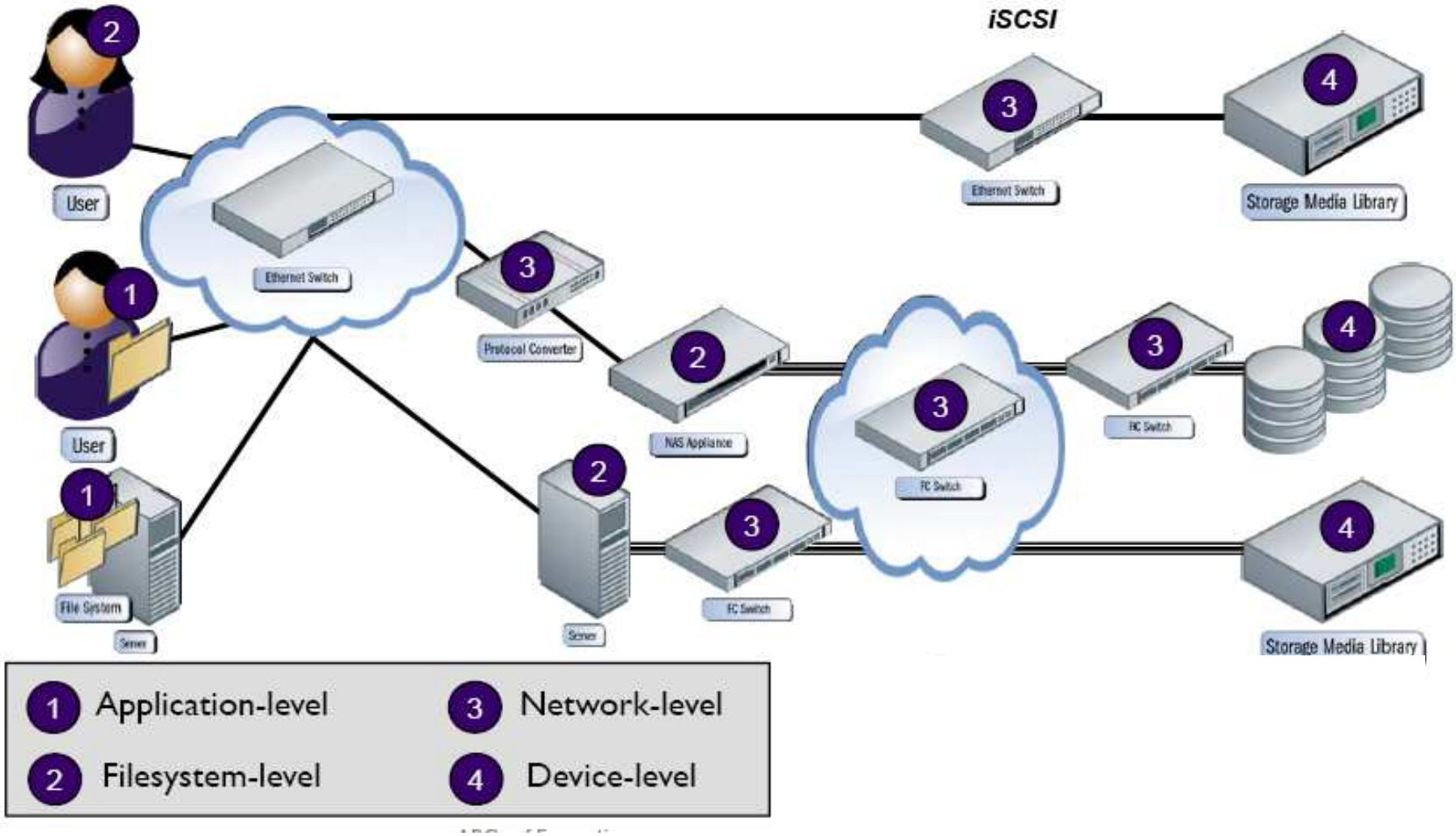
- **Dual control** for access /Separation of duties
- **Restrict access** to cryptographic keys to the **fewest number of custodians** necessary.
- **Store** cryptographic keys securely in the **fewest possible locations** and forms
- **Secure** cryptographic key **storage**: **tamper** responsive cryptographic **hardware**
- Cryptographic **key changes** for keys that have reached the **end of their crypto period** (key rotation)
- Fully document and implement all key-management **processes and procedures** for cryptographic keys.
- Key changes in accordance with recommended crypto periods (ie. **NIST SP800-57**)
- **Audit trails** for all **key management** operations

Sample of Key Management Solution :EKMF



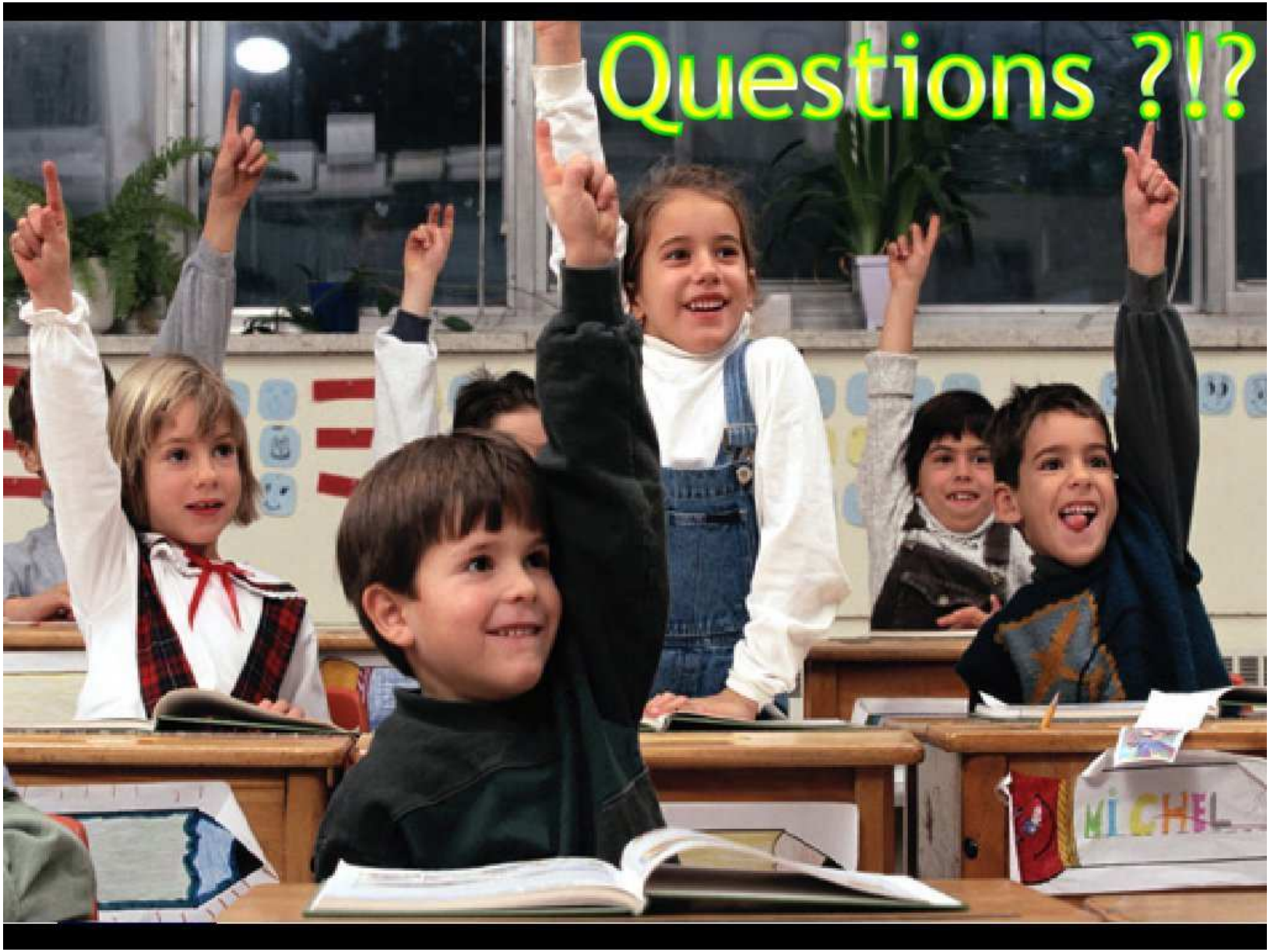
The encryption positioning a difficult choice

Encryption everywhere

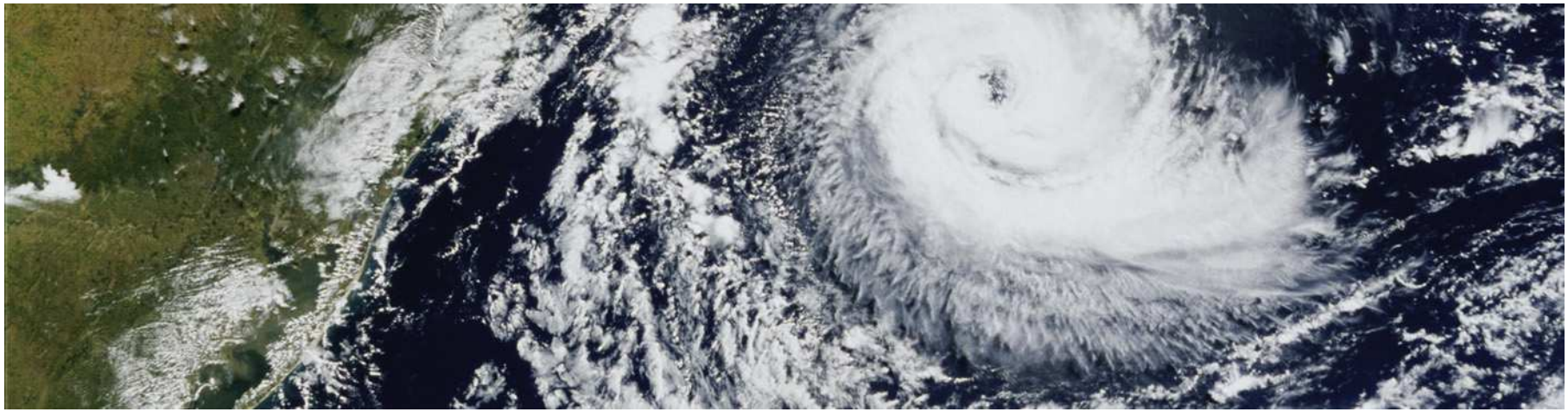


The eight steps method

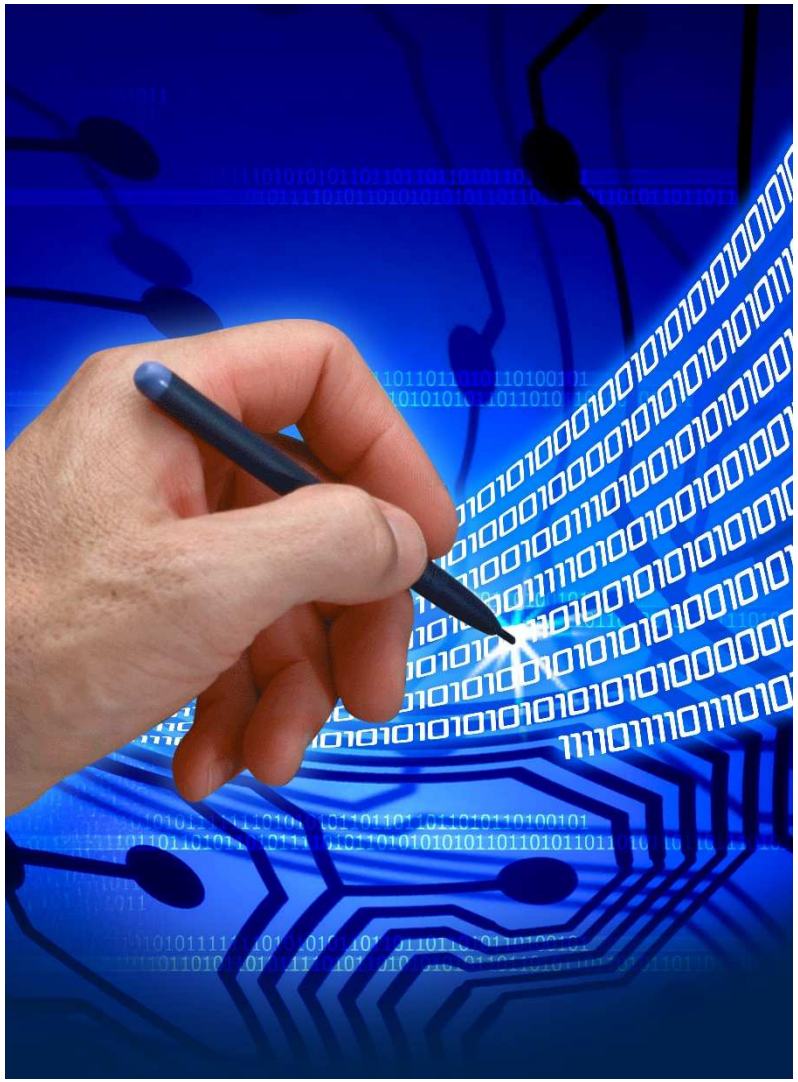
1. **Understand Drivers**
2. **Inventory Data Assets**
3. **Classify Data Assets**
4. **Perform Data Flow Analysis**
5. **Choose Points-of-Encryption**
6. **Design Encryption Solution**
7. **Implement Solution**
8. **Activate encryption**


Questions ?!?

Public Key Infrastructure Overview



Acronyms

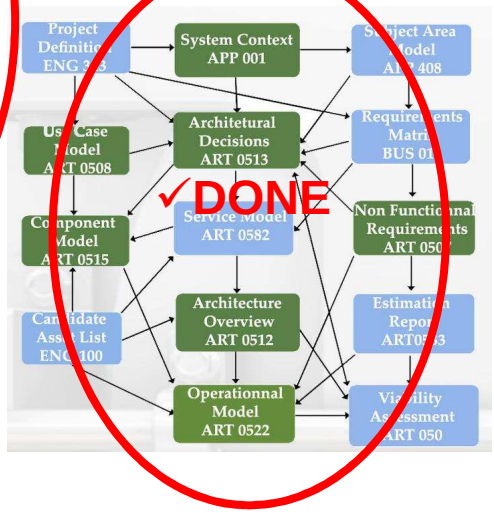


- PKI : public key infrastructure
- CA : certification authority
- RA : registration authority
- CP : certification policy
- CRL : certificate revocation list

Understand the needs and process of a complete PKI Solution

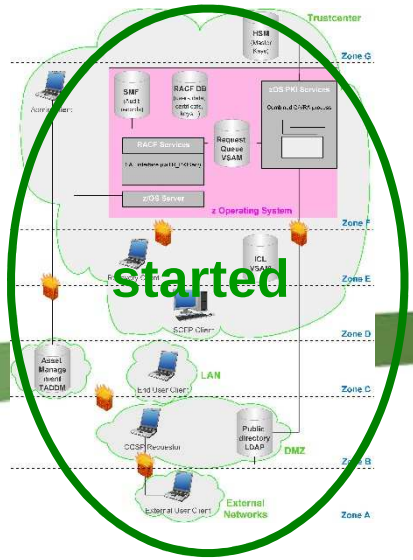
✓DONE

Architectural study



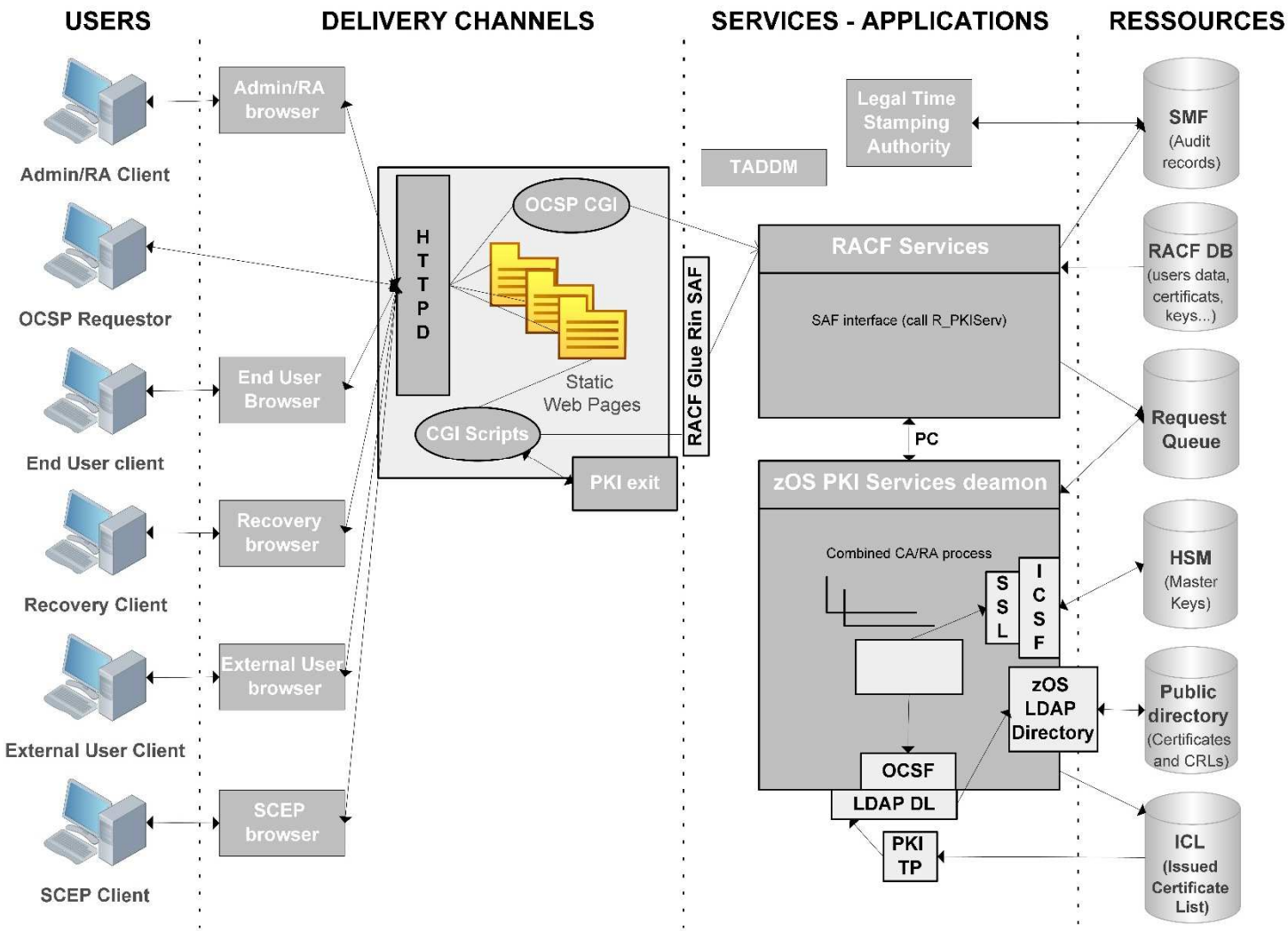
✓DONE

End to end solution on System z



started

Architectural diagram



PKI Public Key Infrastructure definition

- Infrastructure upon trust
- Assures the establishment of a trust link between several entities in communicating entities
  - PKI offers a security solution for electronics exchanges
- In this purpose, PKI produces reliable guarantees before, during and after the exchange. Those guarantees are made with the digital certificates
  - PKI allows to create, manage, store, distribute and revoke digital certificates

The most famous: VeriSign Open Trust

VeriSign™
The Internet Trust Company℠

	Secure Site Pro with EV >>	Secure Site with EV >>	Secure Site Pro >>	Secure Site >>
Buy now	BUY	BUY	BUY	BUY
Renew	RENEW	RENEW	RENEW	RENEW
Trust level	★★★	★★★	★★☆	★★☆
Green address bar	✓	✓		
Extended validation	✓	✓		
VeriSign Secured® Seal	✓	✓	✓	✓
Full organization authentication	✓	✓	✓	✓
Security level	★★★	★★☆	★★★	★★☆
Encryption strength	128-bit minimum to 256-bit	40-bit minimum to 256-bit	128-bit minimum to 256-bit	40-bit minimum to 256-bit
NetSure extended warranty	$250,000	$100,000	$250,000	$100,000
Express delivery			✓	
1-year validity	$1,499	$995	$995	$399
2-year validity	$2,695 *Save over $300*	$1,790 *Save $200*	$1,790 *Save $200*	$695 *Save over $100*
3-year validity			$2,480 *Save over $500*	$995 *Save over $200*
Volume discounts	Save up to 19%	Save up to 19%	Save up to 17%	Save up to 17%

Cost

- Price by certificate : 50 to 800$; Price differs depending on the provider, the period of validity, the cryptography level, the requested functions, and the insurance coverage in case of fraud
- We can estimate a rough average price to be around 250$
- Sample of certificates from VeriSign : 399$ to more than 2600$

Three major challenges for a PKI

Security

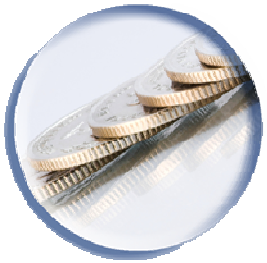
- Needs to ensure the entity's authentication during a communication
- Requirements to guarantee the confidentiality, the integrity and the non-repudiation of the exchanges

Legal

- Must be compliant with all the legal requirements
  > Increasingly complex and difficult
- Must be able to respond to the official auditing company requests

financial

- Utilisation of digital certificates in every exchange and deal
  > significant cost

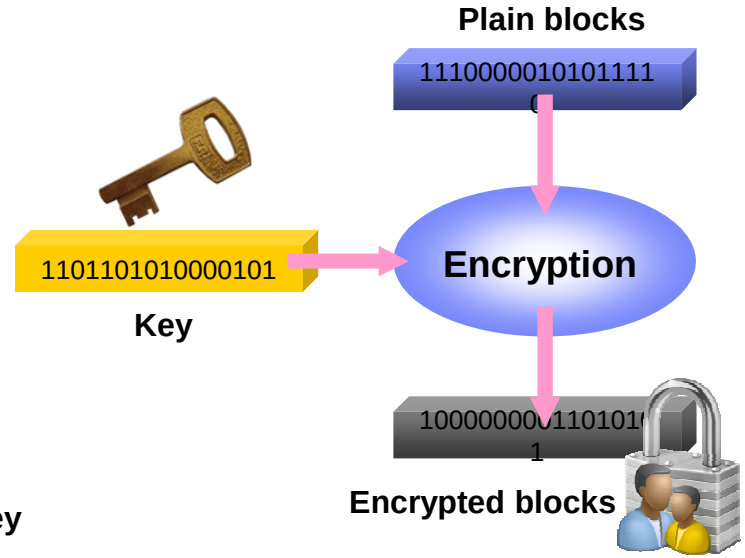


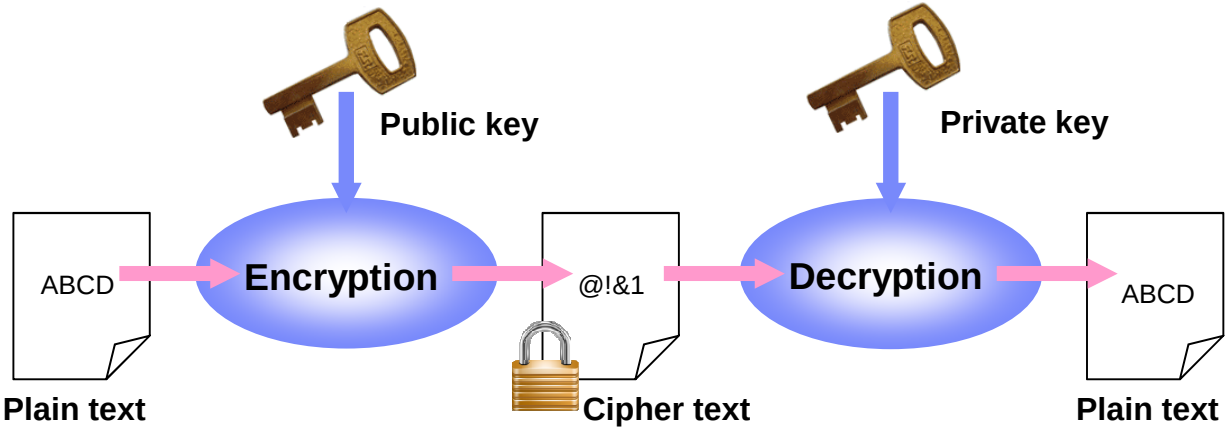
Four security usages

- Authentication
  - Something I know (ex : password)
  - Something I own (smart card)
  - Something which characterizes me (digital signature, fingerprints)
- Integrity
  - Check at the receipt of the document that data aren't corrupted; The transmitter trace must be the same as the receiver trace.
- Confidentiality
  - Encode data during the exchange, thanks to asymmetrical cryptography
- Non repudiation
  - Keep proof of exchanges (digital signature)

Asymmetrical cryptography

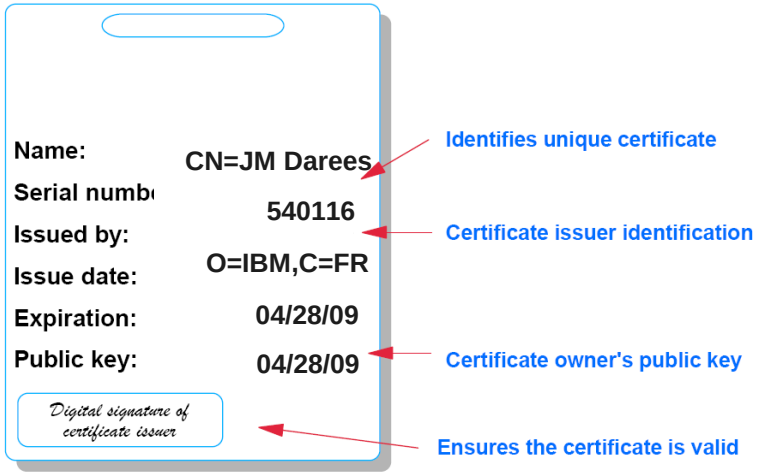
- Secret key public algorithm
- Uses a pair of private and public keys
  - Can't be derived from each other
  - Data encrypted with one key can only be decrypted with the other one

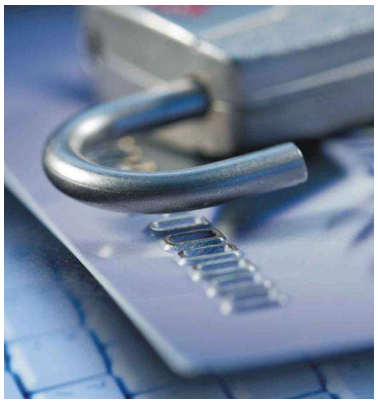




What is a Certificate ?

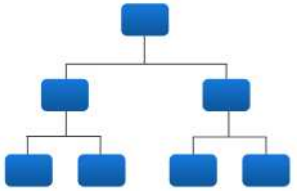
- Digital document that gives evidence that a public key belongs to whom it may concern. It contains at least the information listed below:
  - Public Key
  - Certificate owner's Identity
  - Expiration Date
  - Signature from a third party
  - An utilization type





- Data which can be manipulated by computers
- Based on a norm : X509
  - Universal understanding and utilisation

X.509 Certificates



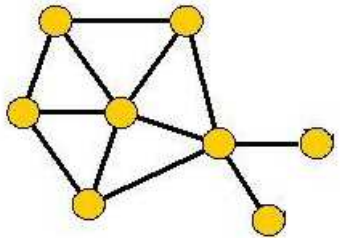
- X.509 Certificates use LDAP-style Distingished Names:
  "CN=Name, OU=Dept, O=Company, C=Country"

- Typical X.509 Certificates contain:
  - Version: The certificate version.
  - Serial Number: Unique identifier for the certificate.
  - Issuer: The entity that verified the information and issued the certificate.
  - Valid-From: The start date.
  - Valid-To: The expiration date.
  - Subject: The person, or entity identified.
  - Public Key: The public key.
  - Extensions: Used to store additional information.
  - Signature Algorithm: The algorithm used to create the signature.
  - Signature: The digital signature from the issuer.

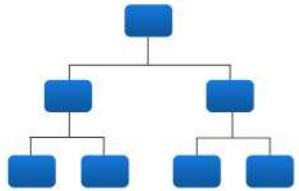
OpenPGP Certificates

- OpenPGP Certificates use User Ids that can consist of a name, a comment, and an email address:
  "Name (Comment) <user@host>"

- Typical OpenPGP Certificates contain:
  - Public key packet: The primary public key for this certificate, creation date, expiration date, packet version, algorithm
  - User ID packet: Name, comment, and an email address.
  - Signature packets: Self signature binding the user ID to the Primary Key, signatures made by other keys, algorithm, Key ID, version number, creation date, signature class
    - Various attribute sub-packets such as preferred algorithms sub-packets, key flags, features and key server preferences.
  - Subkeys: Public sub-keys, version, algorithm, creation date, expiration date
  - Subkey Signatures: Signatures made by the Primary Key to bind the Subkeys to Primary Key.
    - Various attribute sub-packets such as preferred algorithms sub-packets, key flags, features and key server preferences.

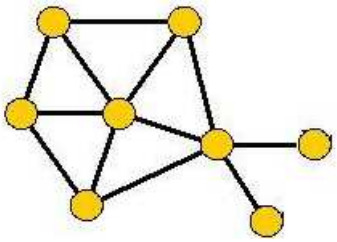


X.509 vs. OpenPGP Certificates



- X.509 uses a hierarchical authentication model
  - Each X.509 certificate contains 1 digital signature, either self signed or signed by a CA
  - A root Certificate Authority (CA) is established and trusted as a self signed certificate
  - Other certificates are signed by a CA within the hierarchy

- OpenPGP uses a decentralized authentication model
  - Each OpenPGP certificate is self signed and can contain multiple signatures from other keys
  - OpenPGP sub-keys are all signed by the Primary key to bind together the Primary and sub-keys
  - Encryption Facility for z/OS provides an option to sign your OpenPGP certificates with a CA.



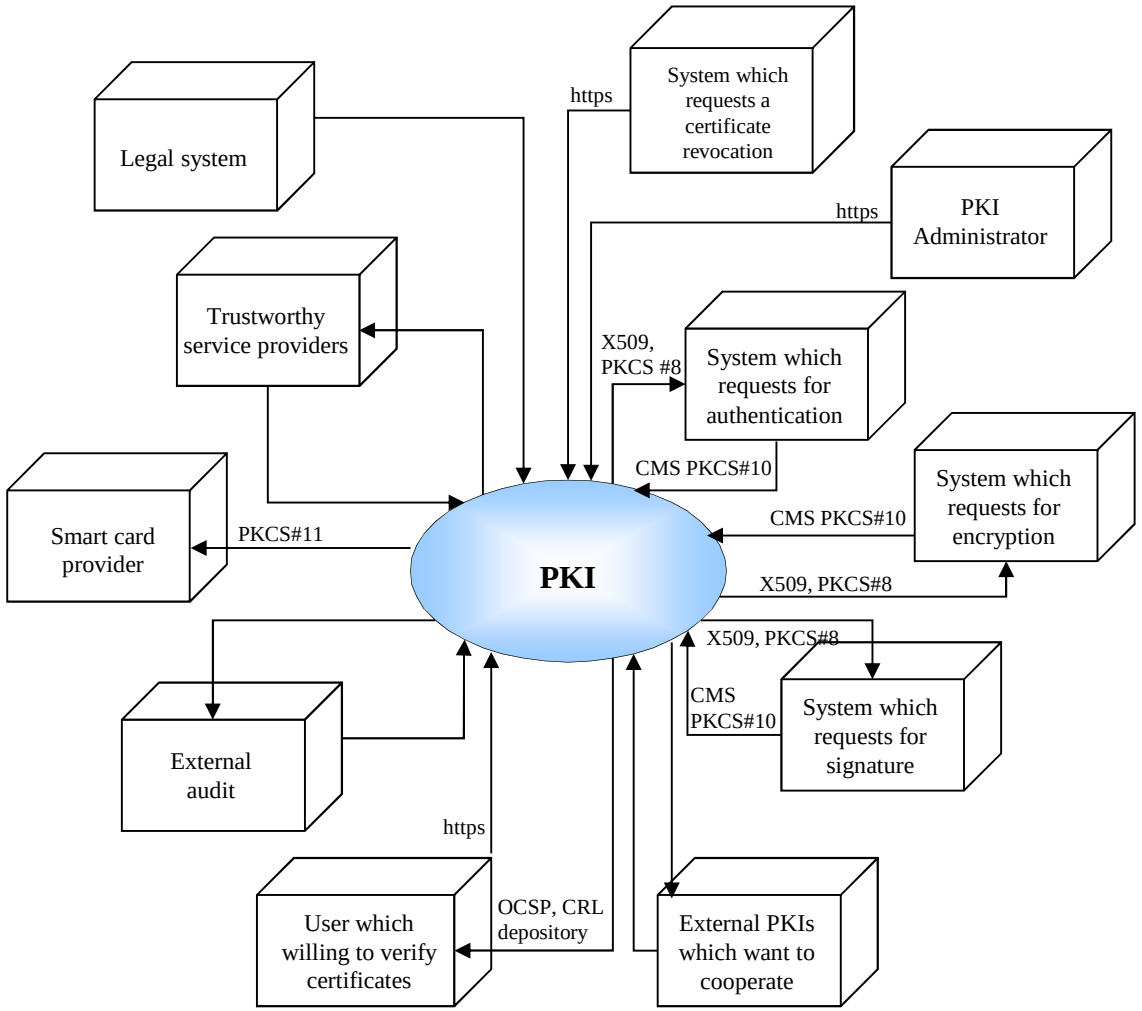
PKI applications samples

- Encryption
  - Provides high confidentiality for the strategic documents exchanges
- Digital signature
  - Reduces paper documents exchanges by keeping the security level required
  - Shortens transportation and processing time
  - Used in Tax Declarations Online, Bills Online for example
  - Used also in Internet Authentication Mechanisms
- In the both cases : use of digital signature and encryption
  - Links upon trust several people in a conversation > Secure exchange
  - Organizes, in a hierarchical way, the access rights for sensitive computing resources
  - Provides Security on the Internet

PKI in business

- Bank
  - Remote access to client account
  - Allocate CB to their clients
  - Online stock exchange
  - E-commerce
- Government
  - Online taxes payments
  - E-passport
  - E-service : health, welfare
- Companies
  - Electronic mail service
  - Authentication to access the computing resources

A PKI communicates



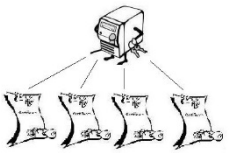
A PKI is never alone

- A PKI is often composed of several CA in order to meet the functional and non functional needs
- Many issues are resolved by the architecture :
  - **Performance** issue when the system grows; One CA may not supply all the users. So such a case a decentralized CA system should be deployed (Hierarchical CA)
  - **Confidence** issue when there is a CA arborescence; To believe in the certificate, the user has to follow the CA path. So if the arborescence grows it may become heavy for users, specially if you have a hierarchical system.
  - **Interoperability** issue when companies have to exchange certificates from different PKIs; Are there agreements between PKIs ?
  - **Evolution** issue when companies want to change the PKI architecture. It is better to plan correctly the evolution capacity/possibilities while designing the PKI architecture solution.

Samples of architectures

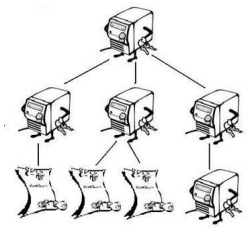
- **Simple architecture**
  - **for companies with limited needs in term of applications and with the same security level for all users**
  - **Flat : a single CA (one confidence domain)**
  - **List of trusted certificates (in web site)**

Use by Windows

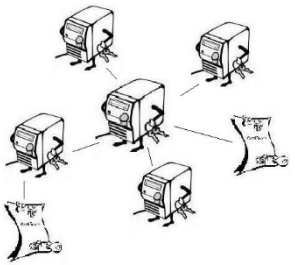


- **Power delegation : certificates are used in several user communities for many applications**

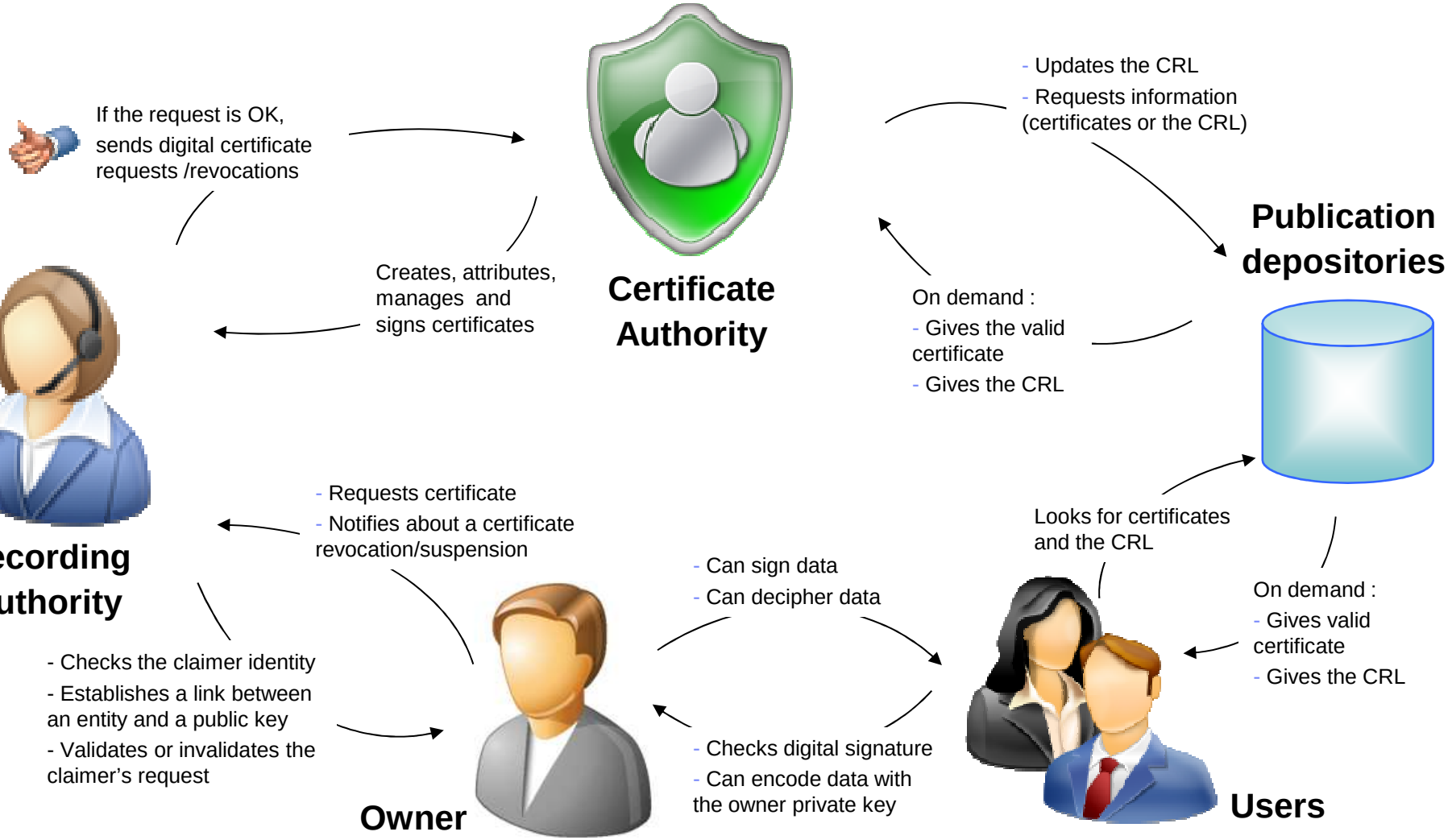
Hierarchy of CAs : pyramid shaped organisation
(CA daughters, CA mothers, CA root) > often used



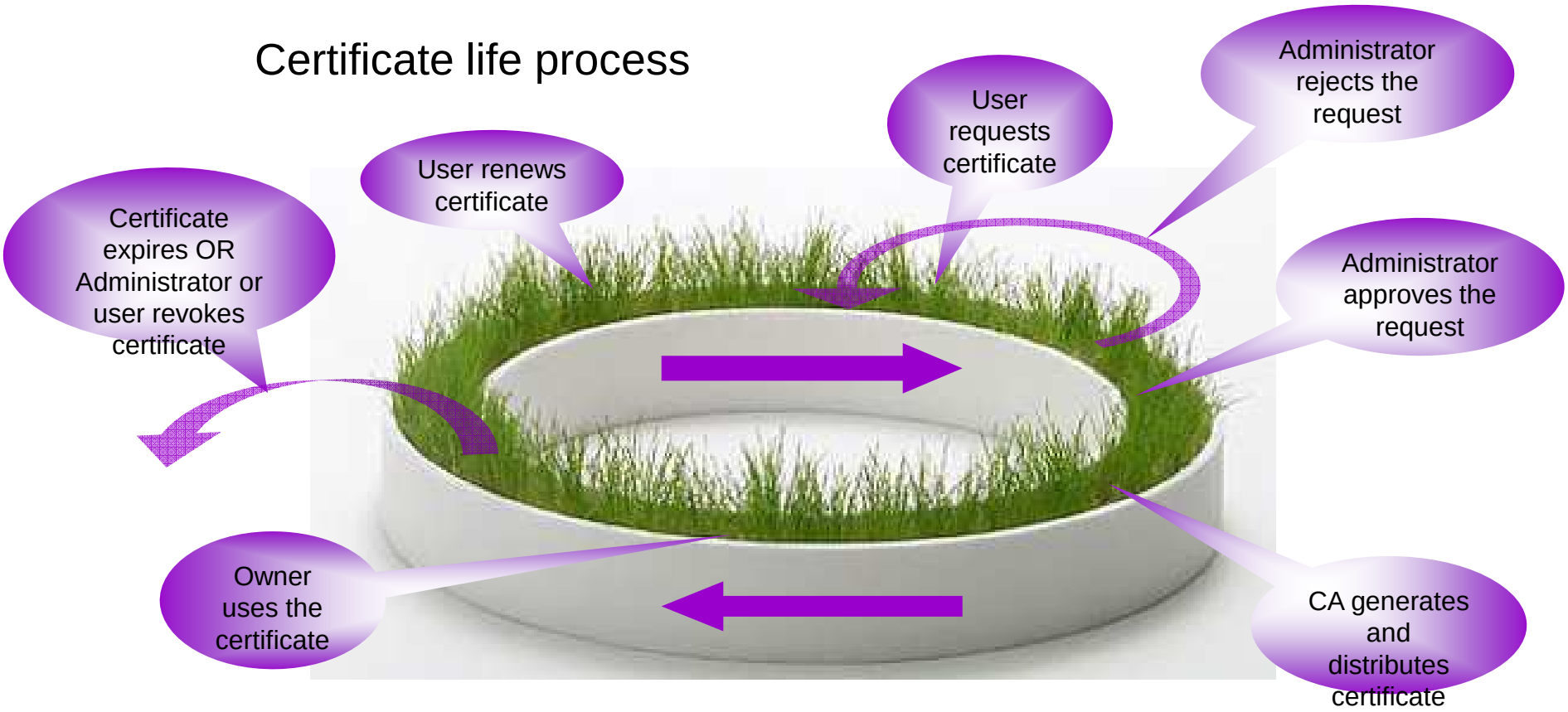
- **Hybrid architecture** : many transactions between different companies > interoperability between PKIs



PKI actors roles, responsibilities and interactions

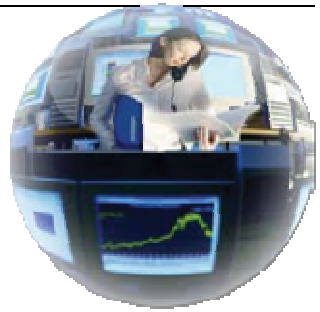


PKI basic processes



- Many other processes can be described like
  - Certificate renewal in case of expiration (or re-validation in case of suspension)
  - Material support Management in case of the CA delivers couple of keys

PKI certification policy



- Why there is a certification policy ?
  - The CP establishes a contract between the PKI and the users
- What is the certification policy ?
  - The CP describes the life cycle of certificates, their utilization rules, the registration by the RA, the way to generate keys, the manner to deliver the certificate, the responsibilities of each entity and the revocation conditions
  - The CP doesn't tell « how to proceed » but just gives the PKI guidelines
  - Owners can find prices of the service and the different responsibilities
  - Decision-Makers analyze the CP to understand the certificates management
  - Users should analyze the supply conditions of the certificates before to rely upon a certificate
  - Auditors have to validate the CP depending on the standards
- The certification policy is established by the Politics Approval Authority

Requirements for a PKI

Technical infrastructure requirements

- Equipments (hosts, crypto cards, smart cards...)
- Software (directory, time-stamping, administration...)
- Takes into consideration interoperability and physical security constraints
- Makes the insertion in the existing context
- The logical structure is an essential component of the PKI architecture

Integration requirements

- Applications have to be able to use the provided certificates
  - Some of them can be modify with simples plug-ins
  - Others like business applications must be changed through development. The development team should have education/ knowledge and communications on PKI solution editor

Requirements for a PKI

Organisation and process requirements

- PKI Organisation and processes must be clearly defined because they differ depending on the PKI structure
- Certificate life cycle management
- PKI components and applications life cycle management

Exploitation requirements

- The PKI must propose an user assistance and an incidents management
- The PKI must take into account future material and software evolutions
- The infrastructure can offer a QoS monitoring and an invoicing service

PKI legal value

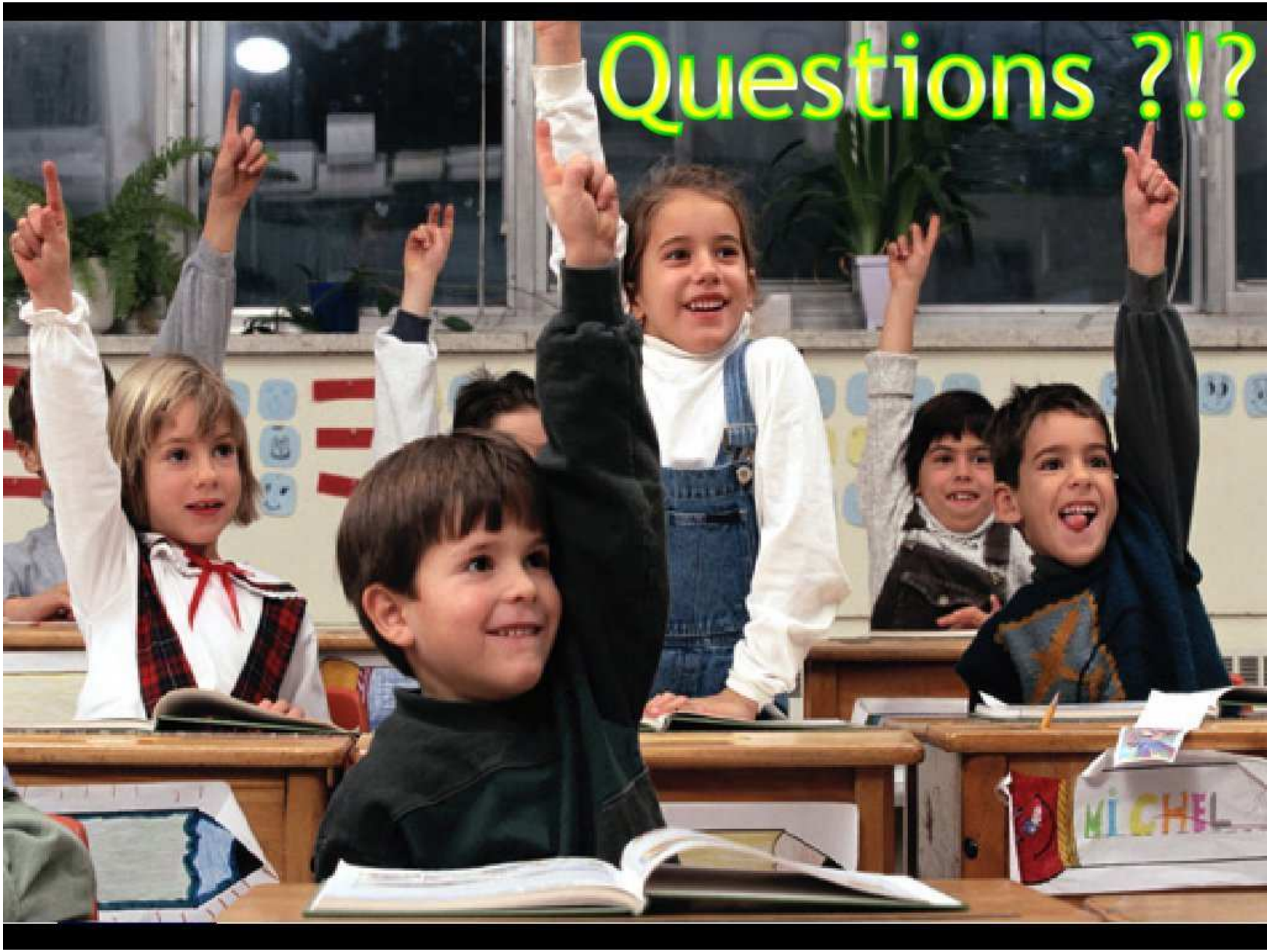
- In the world
  - « European guideline n°1999/93/CE » : Digital signature is equivalent to hand signature
  - The USA has a legislation on digital signature: « Electronic signature in Global and national Commerce Act » (2000); Canada has his one...
  - Must take into account the rules of each country
- Legal specificities according to the project and its functions
- PKI Legal important points
  - User data storage
  - Time-stamping
  - Filing policy necessary to guarantee the security criteria of non repudiation
  - Contract definitions of certificate utilisation
  - Definitions of the certification policy (with the responsibilities of each parties)

Internal or external implementation ?

- PKI insourcing : The PKI solution integrates directly in the company's existing information system
  - The company has already computing resources and will control the whole process
- PKI outsourcing : The company discharges the duty of installing and managing the PKI to service companies
  - The company doesn't own computing resources and/or staff
  - Small or medium companies (not enough staff)
- Hybrid PKI: The company possesses all or a part of the PKI software and hardware resources. An external company houses in the exploitation
- Legal aspect : fairness done by an external audit

Conclusion

- PKI is an important and complex solution
- PKI solution cannot be ignored because of new laws and the large expansion of electronic exchanges
- PKI solution isn't a product but a real infrastructure ! Its implementation, its administration and its management will be decisive in its quality
  returns and the corporate image
- The Keys ceremony is the best way to illustrate this considerable points :
  - This is the process to renew the CA's keys
  - Several entities are needed to renew the CA's private key! Each of them have a part of the secret key. This key is assemble in a secure place and nobody can look the whole new private key …


Questions ?!?