Information Security Principles

Kitisak Jirawannakool

Information Security Specialist

Agenda

- What is Security?
- Security Policies
- Risk Analysis
- Incident Handling
- Physical Security

How it used to be?

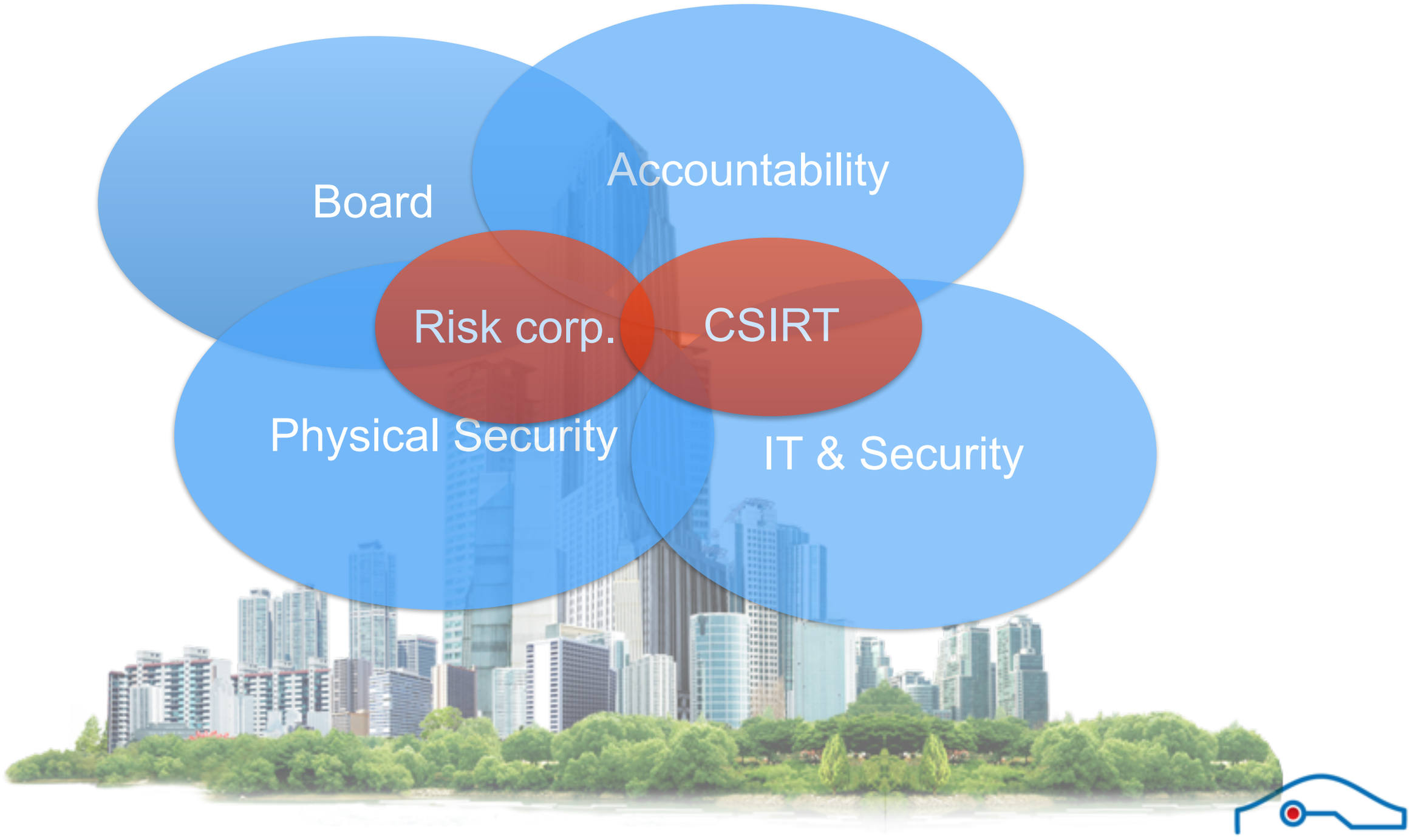
Board

Accountability

Physical Security

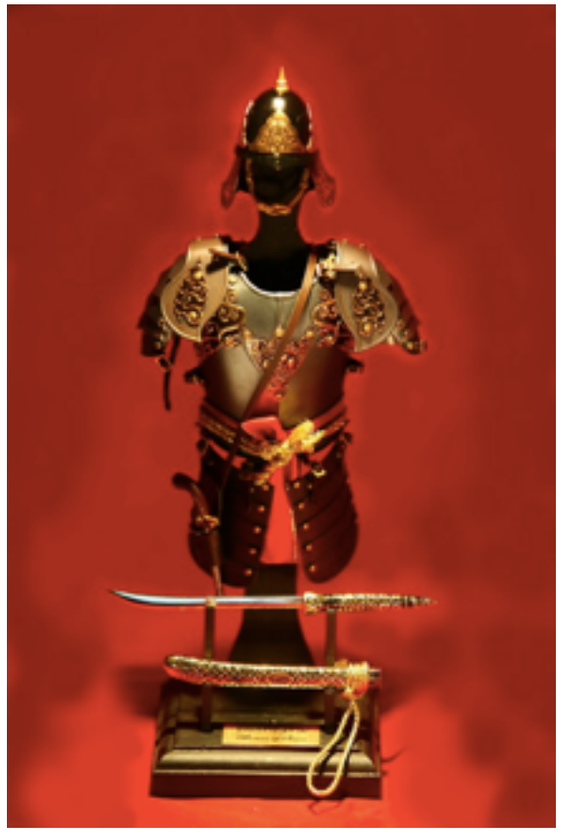
IT & Security

… and How it is growing to be?



What are we protecting?

- What is there to protect ?
  - Primary process
  - Customers, Employees, Identities
  - Products, Contracts
  - Supporting processes
  - Reputation
  - Information, infrastructure
  - Critical infrastructures
  - Health, lives



EGA
e-Government Agency

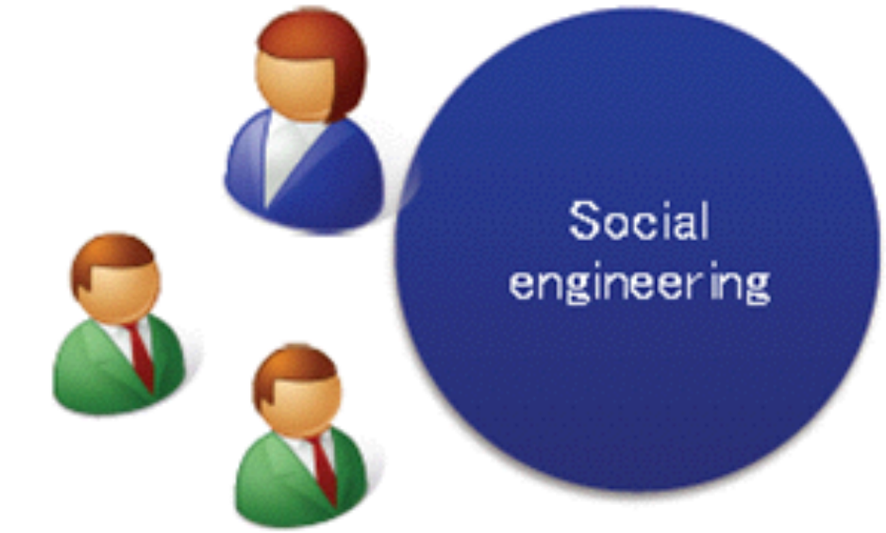
G-CERT by EGA

Situation is changing

* More network devices and users
* More communication opportunity
* More socializing

More chance for attackers
to do their business

Attackers point of view



Technically
Sophisticated
attack

Reach to
information
asset

Important points

Awareness Training

Collaboration

Technical Training

Incident Response

EVER SINCE WE BOUGHT TIMMY A COMPUTER, WE HAVEN'T HAD TO WORRY ABOUT HIM WATCHING ALL THAT JUNK ON TV...

Timmy's Room Keep out!

Internet Porn

Assets

- Hardware
- Software
- Information
- Personnel (People)
- Service
- Location

What is Security?

What is security?

What is security?

What is security?

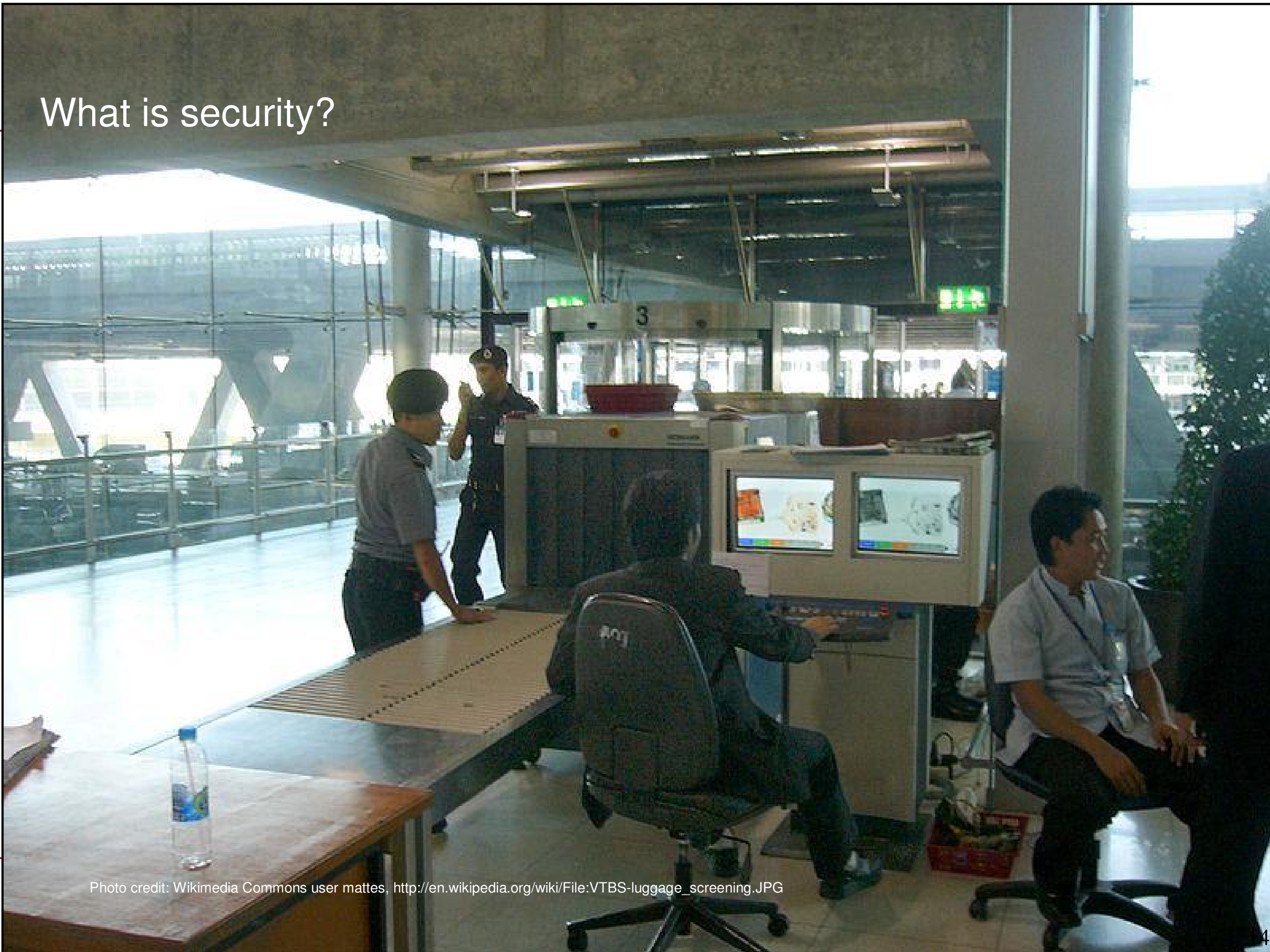


Photo credit: Wikimedia Commons user mattes, http://en.wikipedia.org/wiki/File:VTBS-luggage_screening.JPG

What is security?

Security Goals

- C (Confidentiality)
- I (Integrity)
- A (Availability)

Security Mechanisms

- Authentication
- Access Control
- Encryption
- Signatures

What are attackers' targets?

- Systems
  - OS
  - Software installed
- Network
  - Sniffer
  - Spoofing
  - Flooding / DDoS
- Applications
- Data
- Operation

Security myths: We are not a target

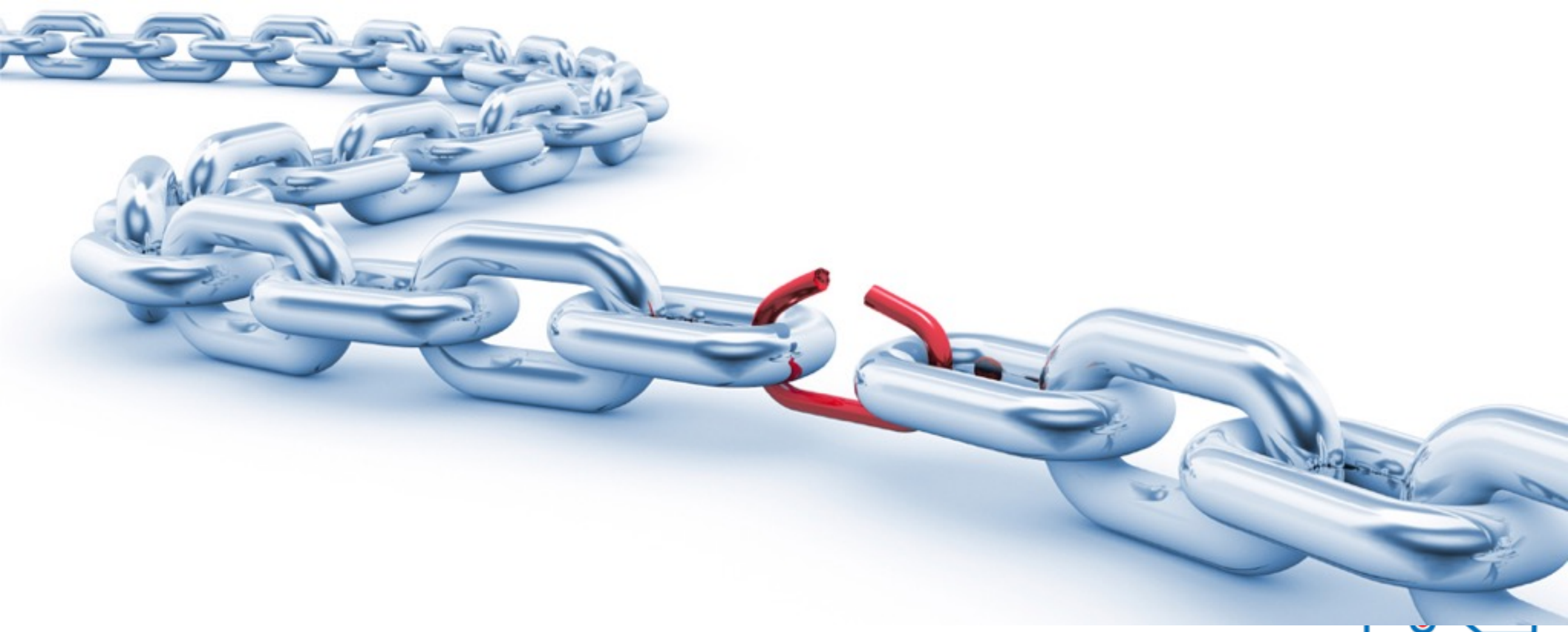
Security Myths : We are not a target

"Mostly I hear it from victims. They think they aren't worth hacking. Some say it's not worthwhile because they're a small business – not on anybody's radar. Others contend they don't collect Social Security numbers, credit card data or other 'valuable' information. They are usually wrong."

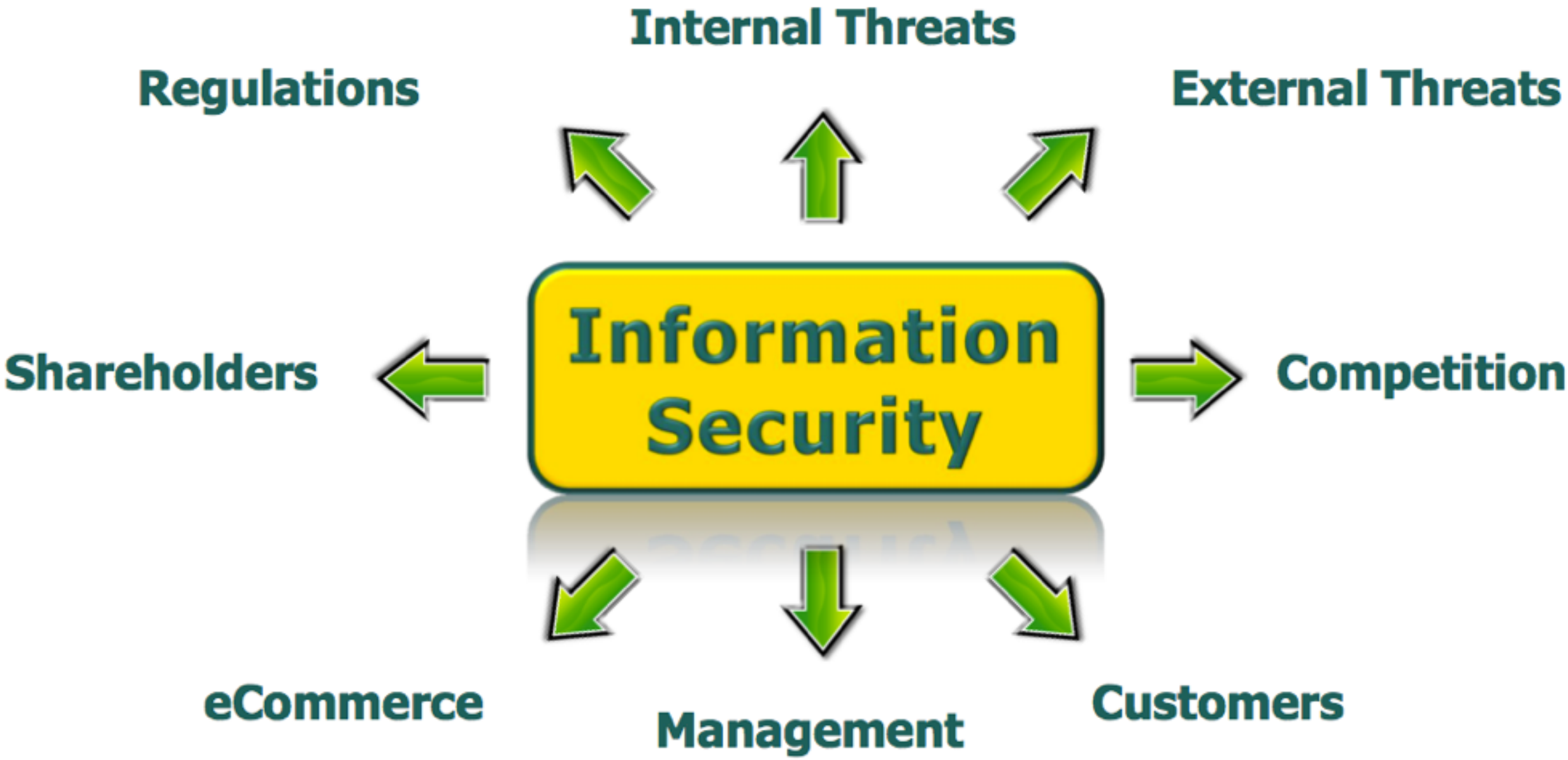
Alan Brill, senior managing director for the cybersecurity and information assurance practice at Kroll

Source: Ellen Messmer, 13 security myths you'll hear -- but should you believe? http://www.networkworld.com/news/2012/021412-security-myths-256109.html

Not be the weakest link



Information Security Today



Security Framework

Organizational Security Policy

Statement by top-level management that security is important to the organization and activities pursuant to a secure state will be recognized, supported, and funded

Functional Policies in Support of Organizational Policy

(these are some examples)

Acceptable Use	Anti-virus	Interconnection
Email Use	Firewall	Host Security
Wireless Use	Extranet	Other Policies

Supporting Mechanisms

Standards
define specific products and mechanisms to be used to support policy

Procedures
define actions to implement standards and baselines

Baselines
define minimum required parameters to achieve a consistent security level

Guidelines
define recommended (yet not required) actions

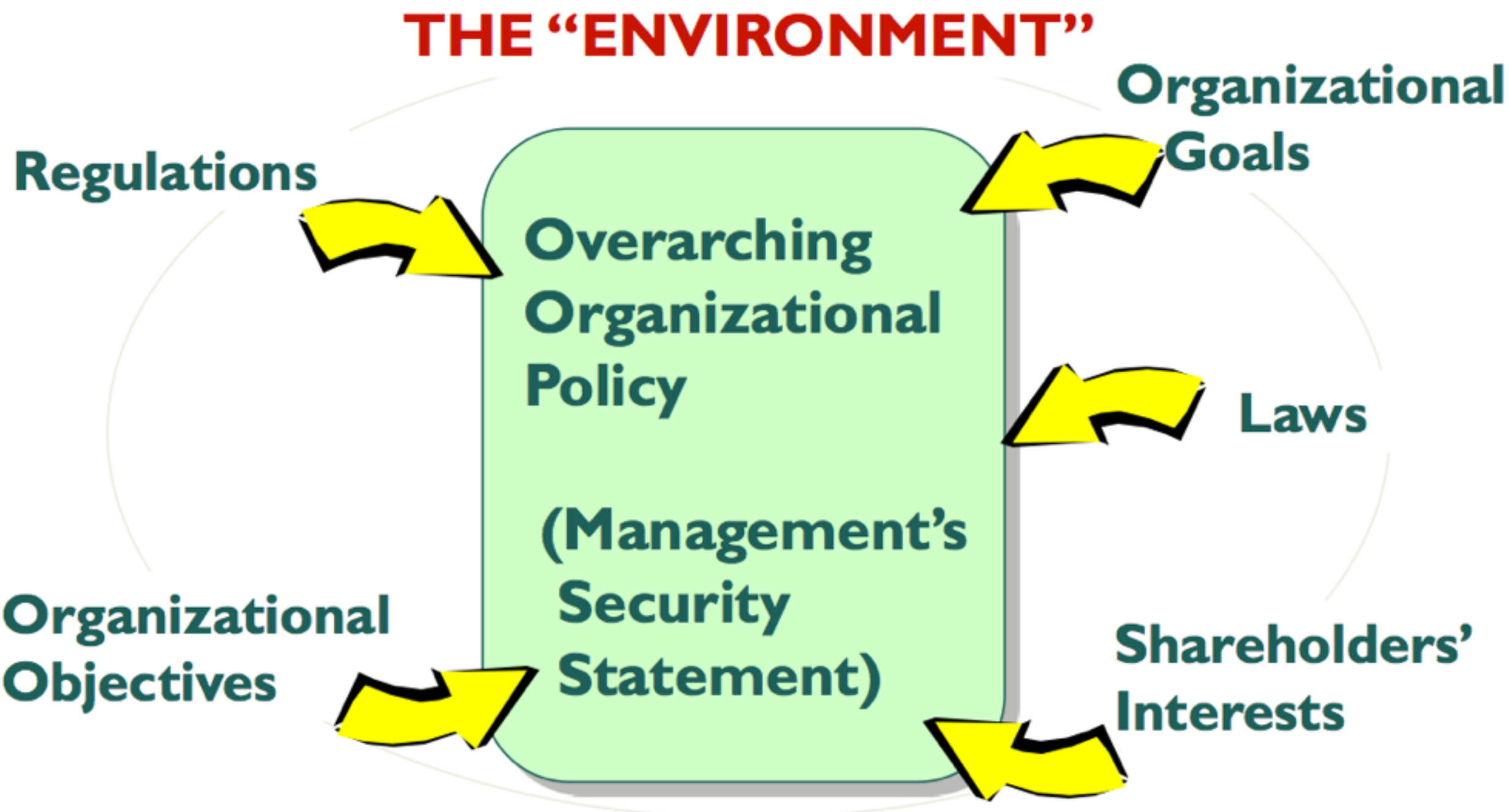
Management's Security Policy

- Provides Management's Goals and Objectives in writing
- Document Compliance
- Create Security Culture

Management's Security Policy

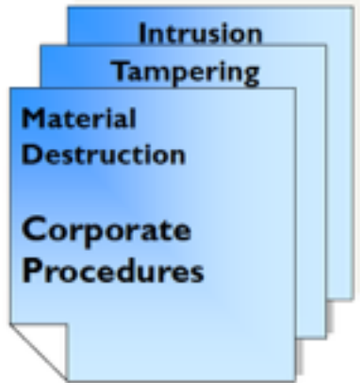
"Security is essential to this company and its future"

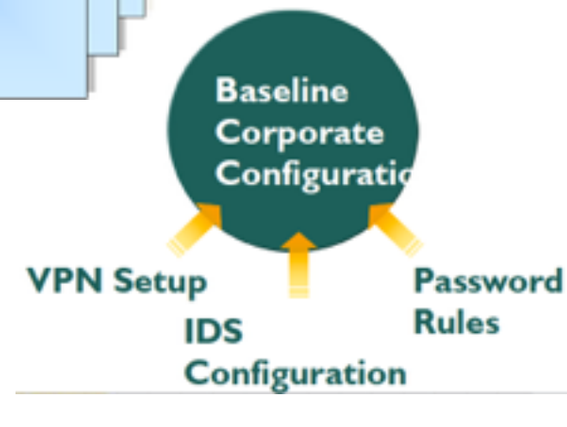
Policy Overview

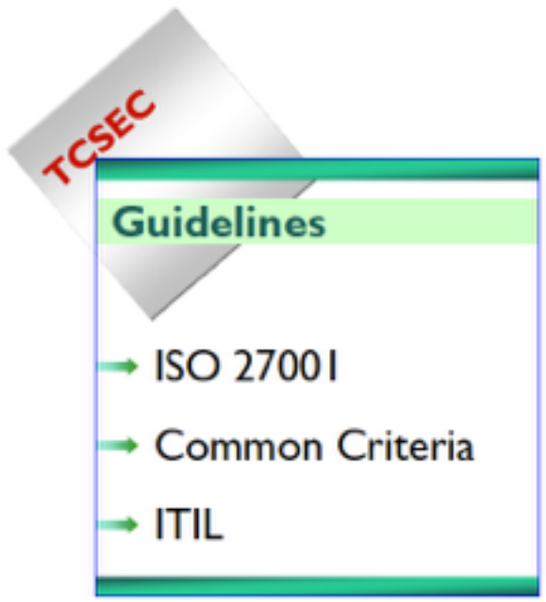


Terminologies

- Procedures
  - Required step-by-step actions
- Baselines
  - Establish consistent implementation of security mechanism
  - Usually platform unique
- Guidelines
  - Recommendations for security product implementations, procurement & planning







PDCA

- New Organization Chart
- Risk Assessment
- Network Design
- Floor plan

Plan

- Policy and Standards
- Countermeasures
- Training Plan

Do

Check

- Security Audit Plan
- Audit procedure

ACT

- Implement new Policies and Standards
- Implement new countermeasures

What is Risk?

- The probability that a particular threat will exploit a particular vulnerability.
- Need to systematically understand risks to a system and decide how to control them.

Pic source : http://www.fiduciarytechnologiesinc.com/files/risk2.jpg

The Elements of Risk

Asset	What we are trying to protect
Vulnerabilities	The weaknesses or faults in our system, processes, awareness or monitoring that could allow an attack to be successful
Threats	The enemy - The forces that may exploit a vulnerability (threat/vulnerability pairing) leading to a successful attack

Risk

Threats

X

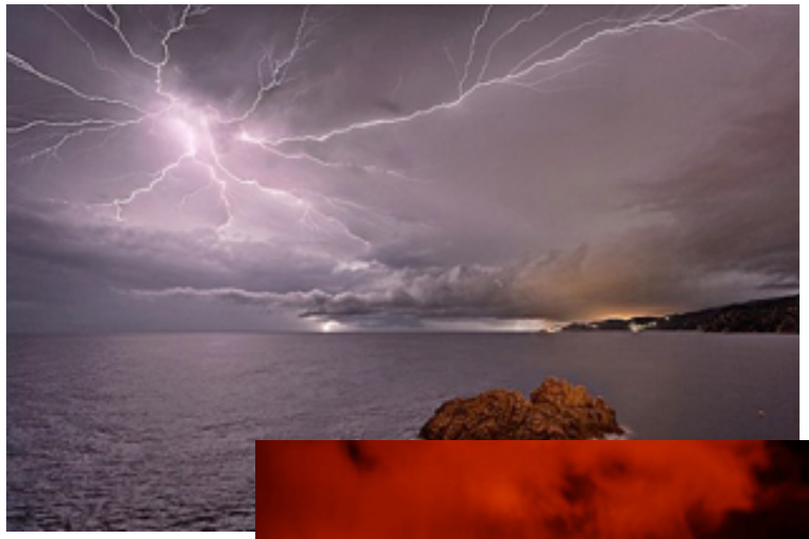
Vulnerabilities

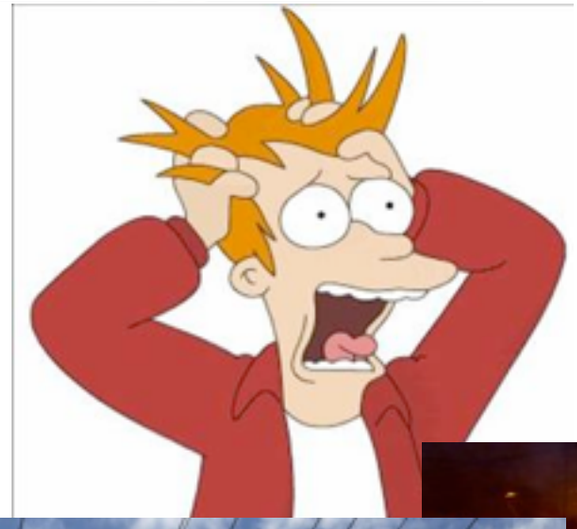
Loss , Damage

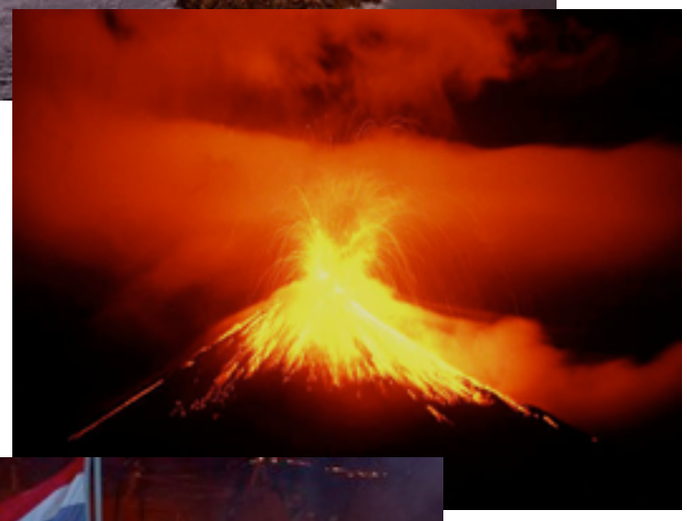
Risks

- Physical damage
- Human interaction
- Equipment malfunction
- Inside and outside attacks
- Data threats
- Application error

Physical threats



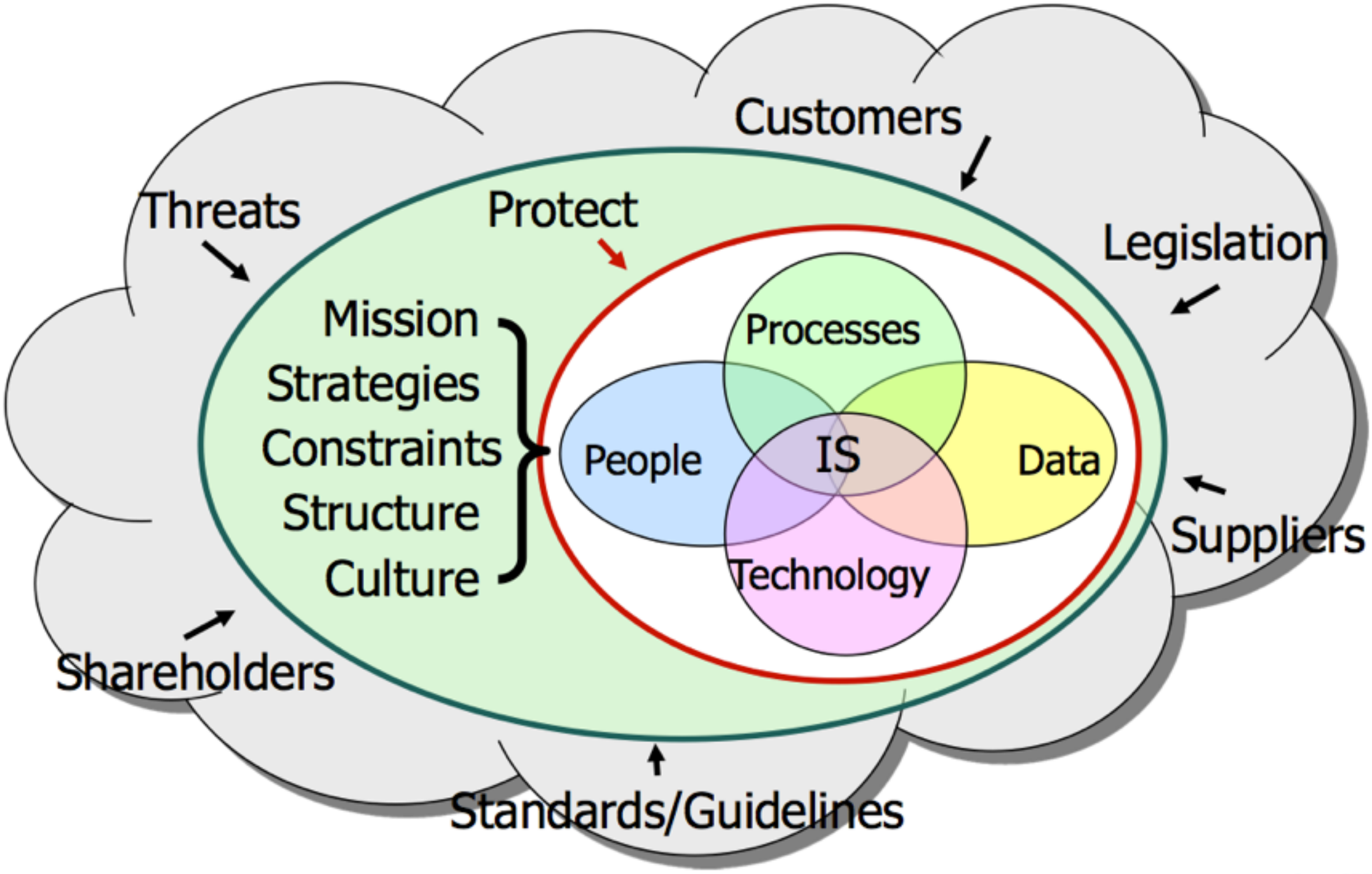




Common Vulnerabilities & Attacks

- Vulnerabilities
  - Network: Protocol manipulation, service misuse, plaintext data
  - Program: Buffer Overflow, Format String Attack
  - Operating System: Unpatched service
  - Process/ Implementation: Weak/ sharing of password
- Attacks
  - Network: Sniffing, Denial of service
  - Program/OS: Malicious code, SQL injection, XSS
  - Social engineering attack

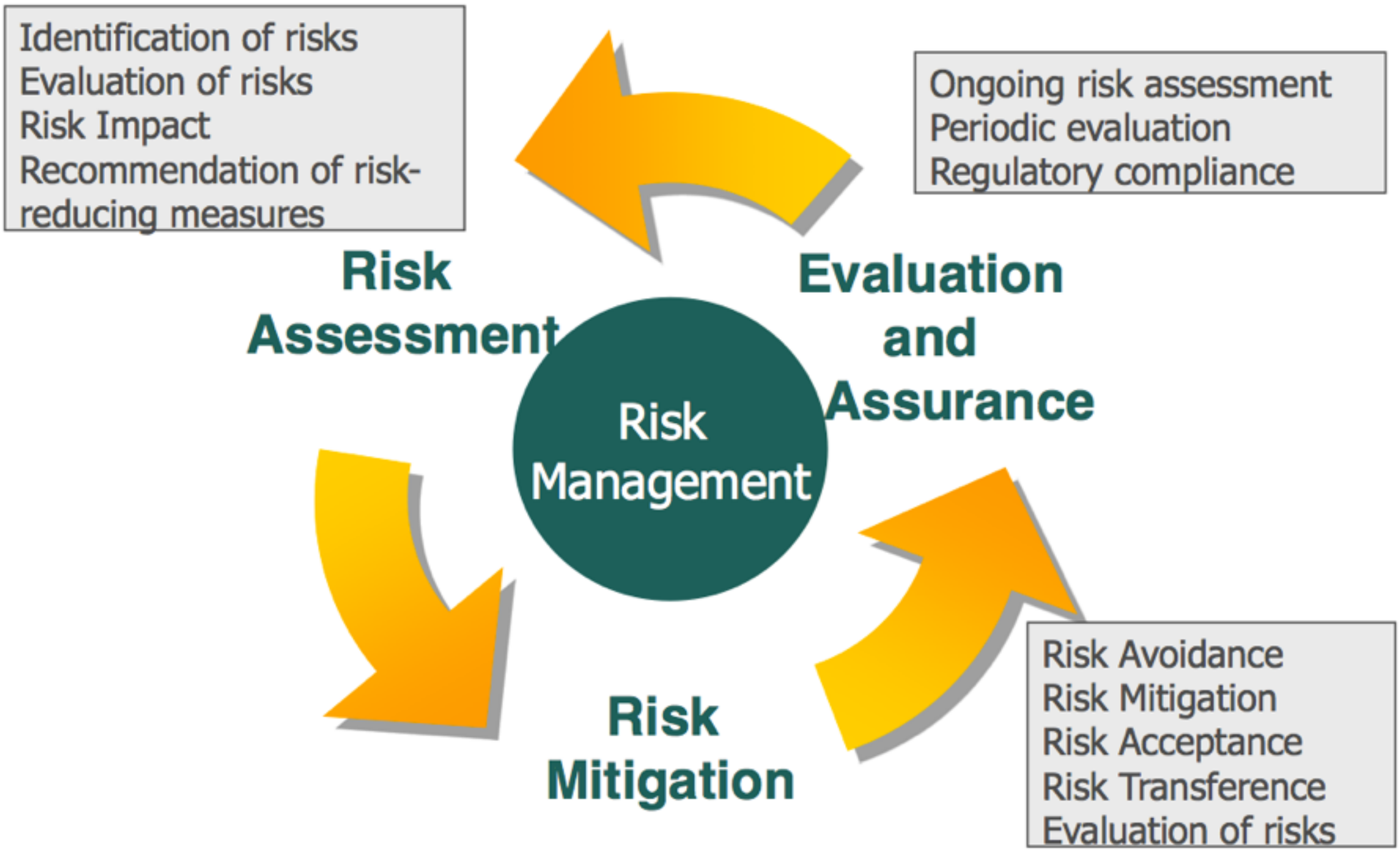
Risk, Response & Recovery



What is Risk Analysis?

- The process of identifying, assessing, and reducing risks to an acceptable level
  - Defines and controls threats and vulnerabilities
  - Implements risk reduction measures
- An analytic discipline with three parts:
  - Risk assessment: determine what the risks are
  - Risk management: evaluating alternatives for mitigating the risk
  - Risk communication: presenting this material in an understandable way to decision makers and/or the public

The Risk Equation



Why Risk Analysis?

- Security risks start when the power is turned-on. At that point, security risks commence. The only way to deal with those security risks is via risk management
- Risks can be identified & reduced, but never eliminated
- The purpose of Risk Analysis is to identify potential problems
  - Before they occur
  - So that risk-handling activities (controls and countermeasures) may be planned and invoked as needed
  - On a continuous basis across the life of the product, system, or project

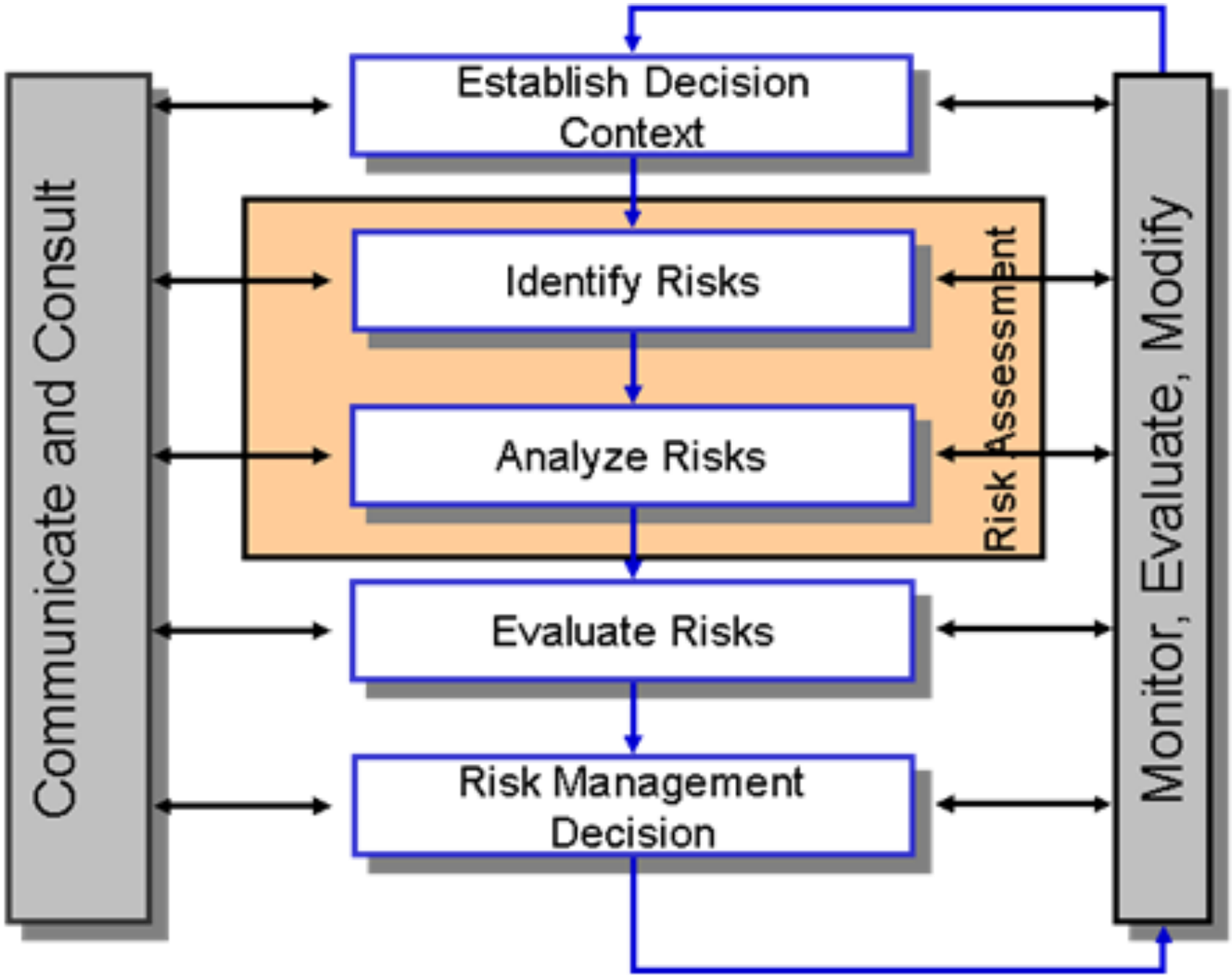
Benefits of Risk Analysis

- Assurance that greatest risks have been identified and addressed
- Increased understanding of risks
- Mechanism for reaching consensus
- Support for needed controls
- Means for communicating results

Key Points

- Key Elements of Risk Analysis
  - Assets, Threats, Vulnerabilities, and Controls
- Most security risk analysis uses qualitative analysis
- Not a scientific process
  - Companies will develop their own procedure
  - Still a good framework for better understanding of system security

Risk Analysis Steps



http://www.corpsnedmanuals.us/DeepDraftNavigation/DDNIncludes/Images/DDNFig2_2RskInfmdDecMkg.png

Risk Management Measurement

Risk Management identifies and prioritizes risks

(Threats, Vulnerability, & Asset Value)

→ TOTAL RISK

Mitigating controls reduce risk:

Total Risk – Mitigating Controls

→ RESIDUAL RISK

- **Residual risk should be set to an acceptable level**

Approaches to Risk Analysis

- Quantitative vs Qualitative Risk Analysis

Quantitative	Numerical Based Data (Hard Data)	Financial data Objective
Qualitative	Scenario Based Data (Soft Data)	Scenario-Oriented Understandability Subjective

- Most organizations will use a hybrid of both approaches to risk assessment.

Who should be Involved?

- Security Experts
- Internal domain experts
  - Knows best how things really work
- Top management level responsible for accepting risks
- Managers responsible for implementing controls
- Asset owners ****

Threats

- An expression of intention to inflict evil injury or damage
- Attacks against key security services
  - Confidentiality, integrity, availability

Vulnerabilities

- Flaw or weakness in system that can be exploited to violate system integrity.
  - Security Procedures
  - Design
  - Implementation
- Threats trigger vulnerabilities
  - Accidental
  - Malicious

How to define causes of Risk?

- Assets selection
- Asset identification
- Threats
- Vulnerabilities

- Depends on what do you concern

Controls/Countermeasures

- Mechanisms or procedures for mitigating vulnerabilities
  - Prevent
  - Detect
  - Recover
- Understand cost and coverage of control
- Controls follow vulnerability and threat analysis

Risk/Control Trade Offs

- Only Safe Asset is a Dead Asset
  - Asset that is completely locked away is safe, but useless
  - Trade-off between safety and availability
- Do not waste effort on efforts with low loss value
  - Don’t spend resources to protect garbage
- Control only has to be good enough, not absolute
  - Make it tough enough to discourage enemy

Risk Example by Asset types

- Hardware
- Software
- Information
- Personnel (People)
- Service
- Location

Hardware

- Asset : Web server
- Threats
  - Hardware failure
- Vulnerabilities
  - Lack of system monitoring
  - Lack of maintenance process
- Controls
  - Monitoring system use (A.10.10.2)
  - Maintenance contract expanded

Software

- Asset : Windows 8
- Threats
  - Use of Pirated Software
- Vulnerabilities
  - Lack of policy restricting staff to use licensed software
  - Lack of user awareness
- Controls
  - Acceptable use of assets
  - Establish formal disciplinary process

Information

- Asset : Confidential files
- Threats
  - Disclosure of confidential information
- Vulnerabilities
  - Lack of information & document classification and handling procedure
  - Lack of Physical security
  - Lack of User awareness
- Controls
  - Establish or implement procedures in information handling
  - Define rules for working in secure areas
  - Information Security Education and Training

Personnel

- Asset : Clerk
- Threats
  - Operational Staff or User Errors
- Vulnerabilities
  - Lack of efficient and effective configuration change control
  - Lack of technical skill
  - Lack of User awareness
- Controls
  - Establish change control management
  - Information Security Education and Training

Personnel (2)

- Asset : Clerk
- Threats
  - Resign
- Vulnerabilities
  - Lack of cross-function / backup staff
  - Poor employee relationship management
- Controls
  - Provide cross-functional training for key job function
  - Management should provide the resources needed

Services

- Asset : Network system
- Threats
  - Failure of communication services
- Vulnerabilities
  - Lack of redundancy
- Controls
  - Arrange backup internet service
  - Use redundant Internet service (two ISPs)

Location

- Asset : Head office building
- Threats
  - Sabotage
- Vulnerabilities
  - Lack of Physical Security
  - Lack of Change Management Controls
- Controls
  - Implement environment threats protection
  - Establish formal physical entry controls
  - Establish change control management

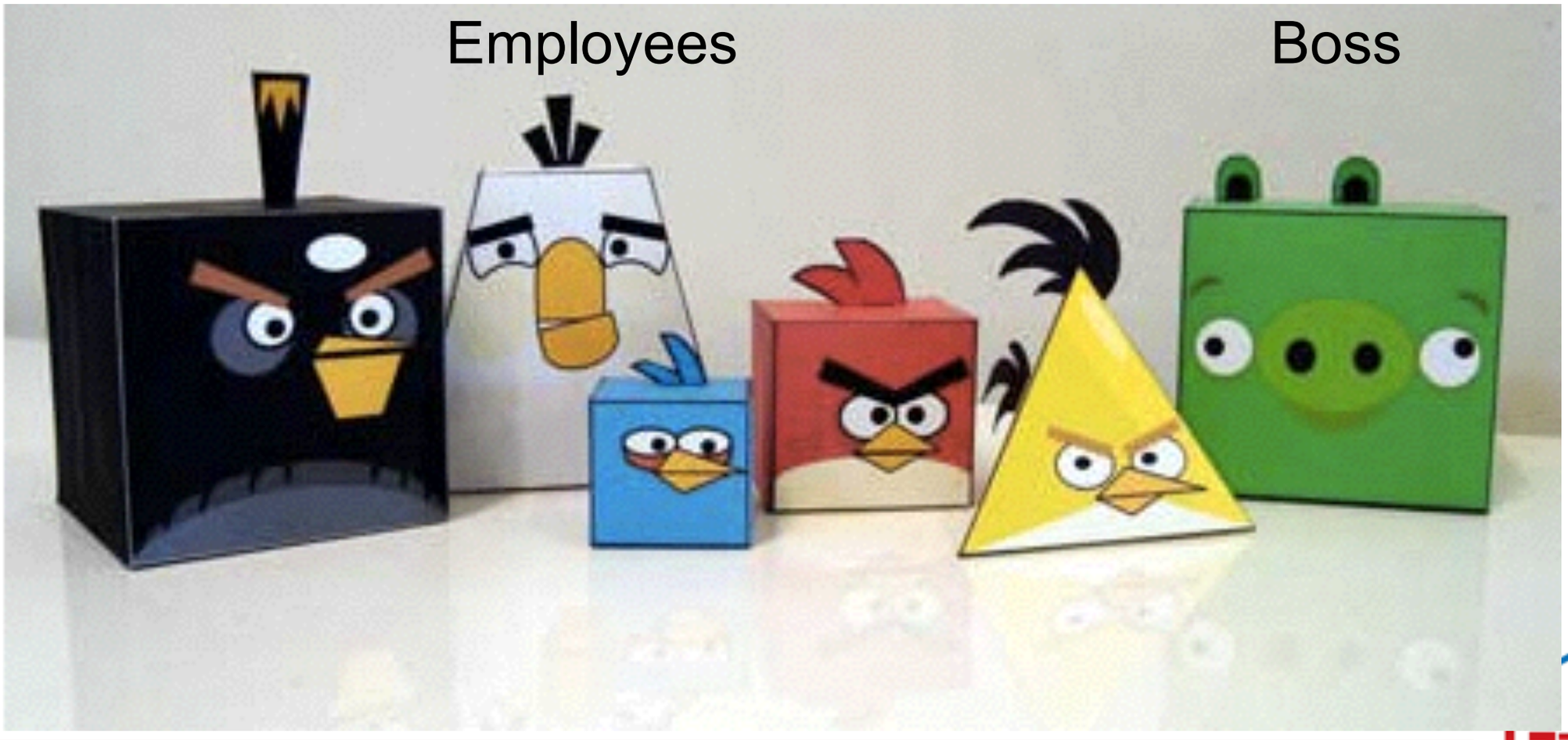
Group Activity#1 - Risk assessment

- Separate into 3 groups
  - IT Support
  - Server/Network Administrator
  - Software/Web Development
- Define your assets in your organization
- Try to think about threats and countermeasure which is possibly related to your assets above
- and present
- 30 minutes

Risk Management

When Risks are happened ....

- What should we do, if we are management level?
- In case of Facebook and Youtube are risks



Risk Management

AVOID

ACCEPT

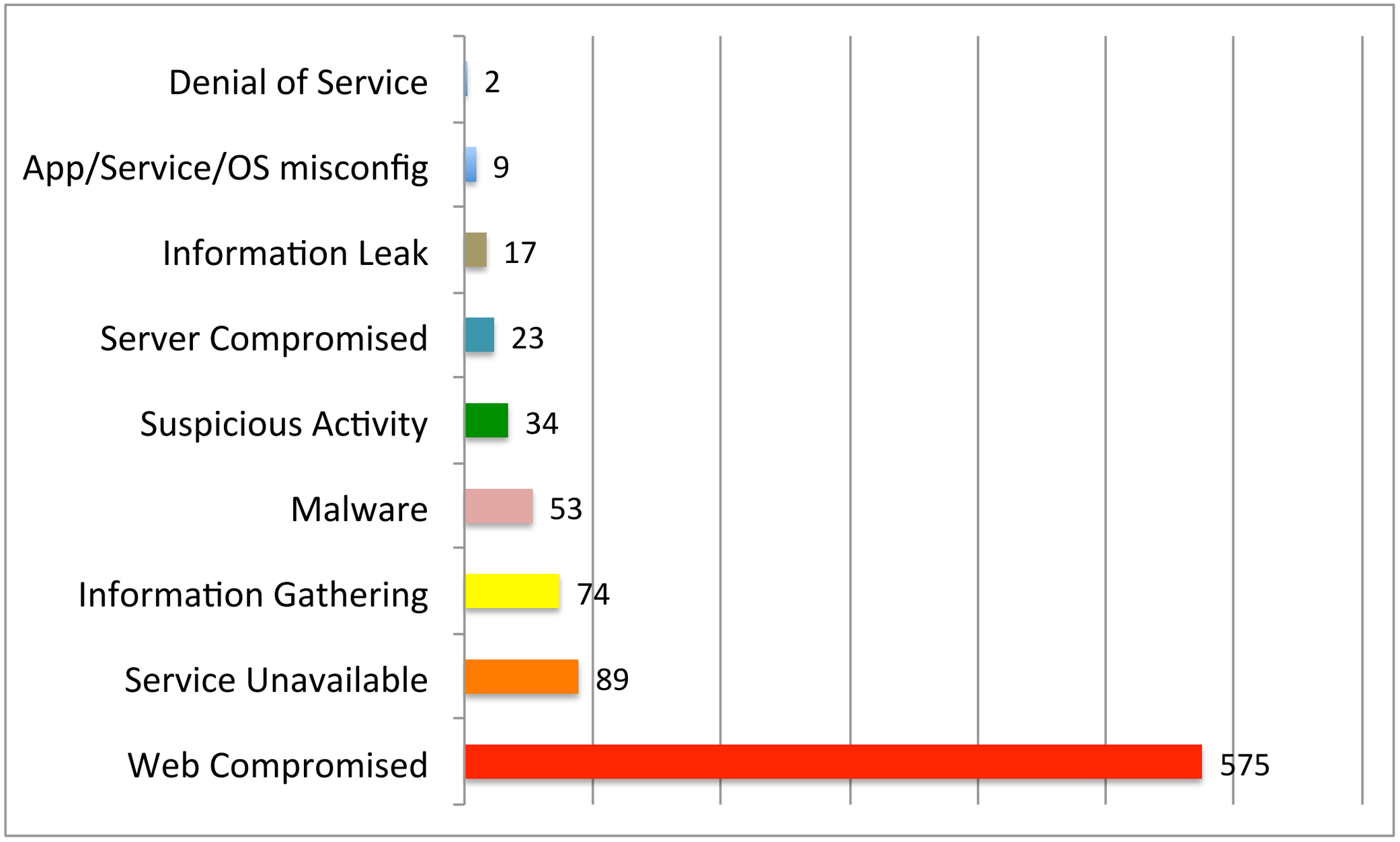
REDUCE

TRANSFER/SHARE

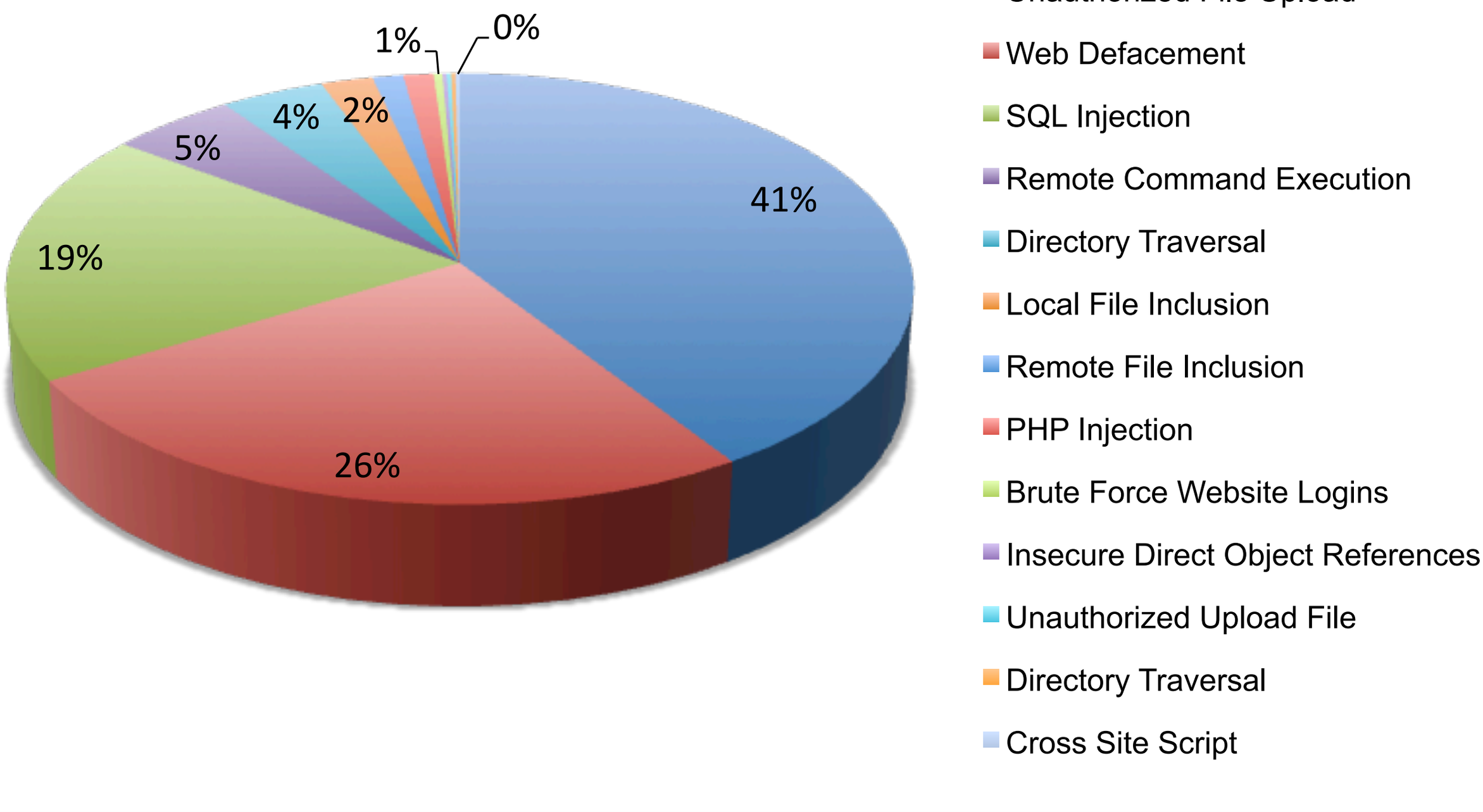
Key to success for IT security implementation

- Supported by CEO or management level
- Implement most suitable IT security tools (both quality and budget)
- Every departments are involved to do risk assessment/analysis
- All of employees have awareness

Incident 2016 (Jan - Jun)



Web attacks by categories



What are we facing recently?

NETCRAFT

Home | News | Anti-Phishing | Security Testing | Internet Data Mining | Performance | About Netcraft

Thai Government websites infested with malware

Nearly 100 Thai Government websites were hacked and used to serve malware last month. More than 500 distinct attacks were launched from these websites, representing about 85% of all government-hosted malware in the world.

Seven of the hacked sites belong to Thai police forces, such as the Narathiwat Provincial Police website at **narathiwat.police.go.th**, where hackers have appended a large chunk of malicious VBScript to the page shown below. This script attempts to write malware from a hexadecimal string to a file named **svchost.exe** on the local file system, and then tries to automatically run the malware contained within the freshly planted executable file.

This page on the Narathiwat Provincial Police website exposes visitors to drive-by malware.

SOFTPEDIA

Softpedia > News

100 Thai Government Sites Hacked, Abused for Malware Distribution and Phishing Attacks

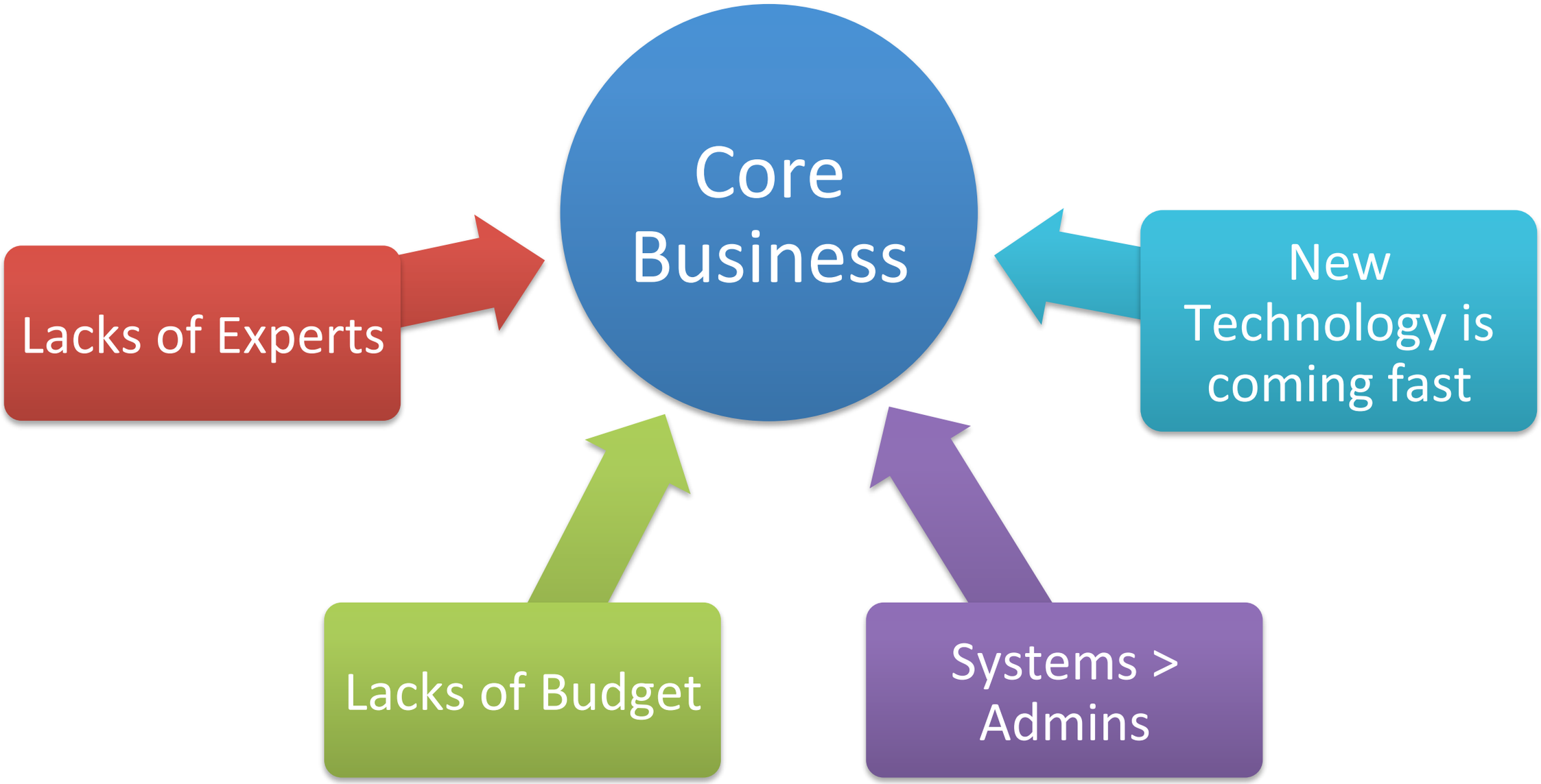
S | COMPANIES | OPINION | POLITICS | TECHNOLOGY | SP

EGA
e-Government Agency

Thai government websites hacked by Islamist group

IANS | Bangkok
August 24, 2015 Last Updated at 14:30 IST

Why?


Core Business
Lacks of Experts
New Technology is coming fast
Lacks of Budget
Systems > Admins

Threat Landscapes

- Exploitation
- Web application hacking
- Botnet
- Malware/ Ransomeware
- Phishing/ Spear Phishing
- Port scanning
- Brute force (Login attempts)

- anything else?

Exploitations

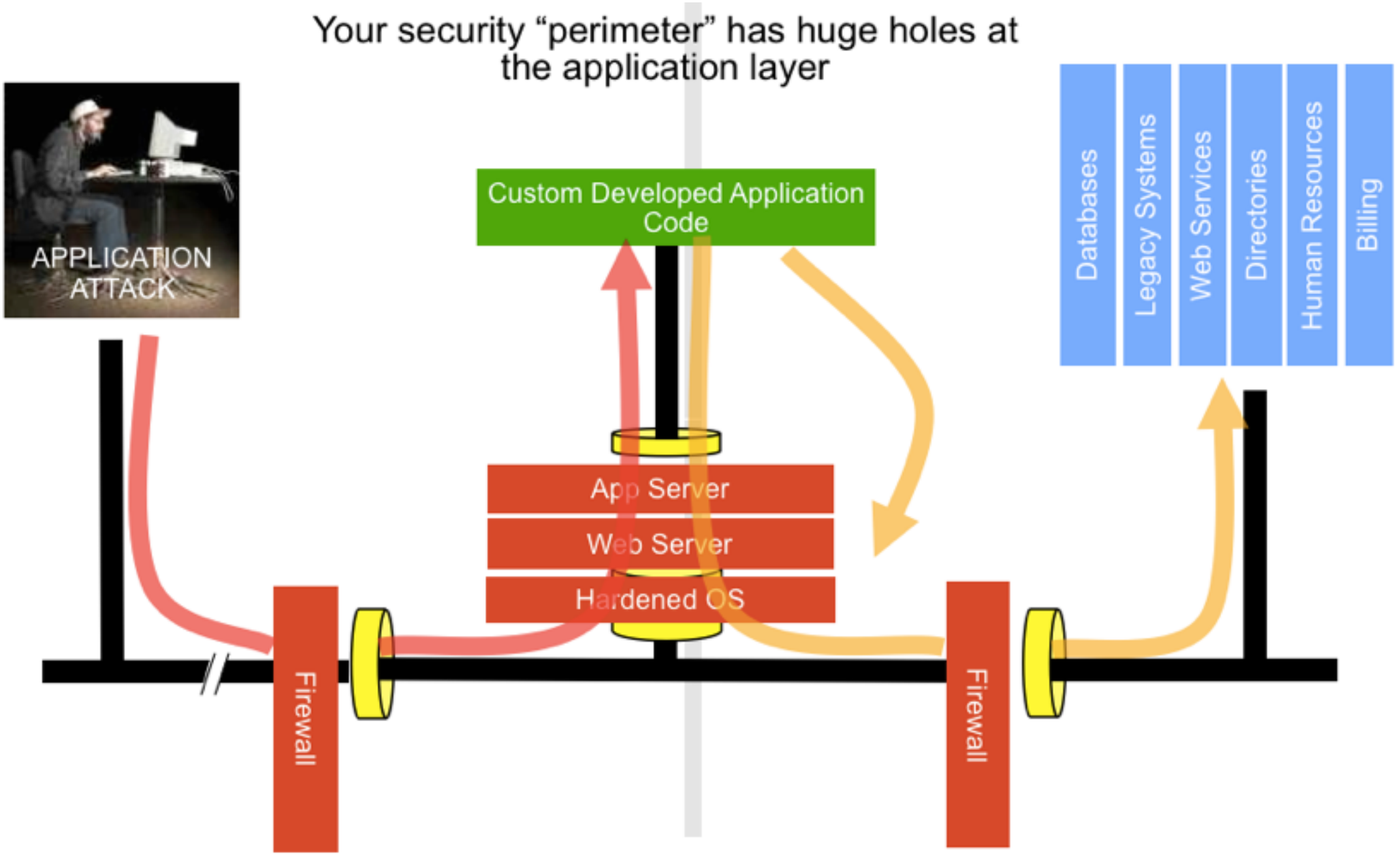
- Target on 0-day vulnerabilities
- Heartbleed
- ShellShock

```
root@ubuntu:~# env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

Web Attacking

- Web Defacement
- Malicious script spreading
- Phishing
- Database and Credential stolen

Why we need web application security?



Network Security is not enough

- Network Security Mostly Ignores the Contents of HTTP Traffic, such as....
  - Firewalls, SSL, Intrusion Detection Systems
  - Operating System Hardening, Database Hardening
- Need to secure web application (Not Network Security)
  - Securing the "custom code" that drives a web application
  - Securing libraries
  - Securing backend systems
  - Securing web and application servers
- **Cloud Computing is coming**, the infrastructure is secured by the provider but we are still need to secure our application.

OWASP

- Open Web Application Security Project
- http://www.owasp.org
- Open group focused on understanding and improving the security of web applications and web services!
- Hundreds of volunteer experts from around the world

OWASP
The Open Web Application Security Project
http://www.owasp.org

OWASP

The Open Web Application Security Project

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

Reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls

Main Page

Welcome to OWASP

the free and open application security community

- OWASP Summit 2011
- Top Ten
- WebScarab
- ESAPI
- ASVS
- AntiSamy

About • Searching • Editing • New Article • OWASP Categories

The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

You'll find everything **about OWASP** here on our wiki and current information

Special

Quick Reference

Election of Officers Upc

Community Forums - C

Contact OWASP Staff -

Industry Citations - Cli

Podcast - Listen Now

Blog - Click Here

EGA e-Government Agency

G-CERT by EGA

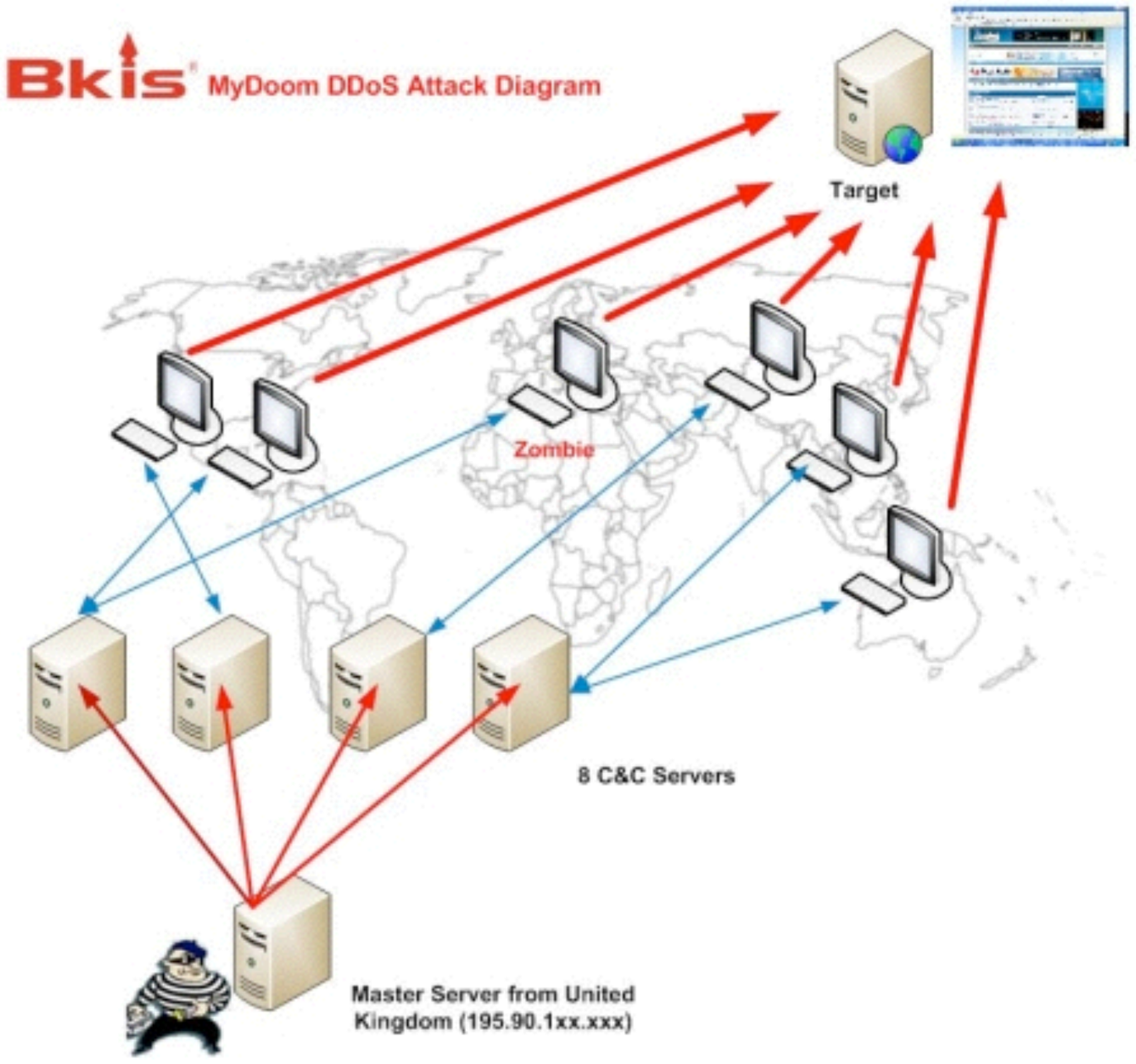
OWASP Top 10 2013

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting(XSS)
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery(CSRF)
- Using Components with Known Vulnerability
- Unvalidated Redirects and Forwards

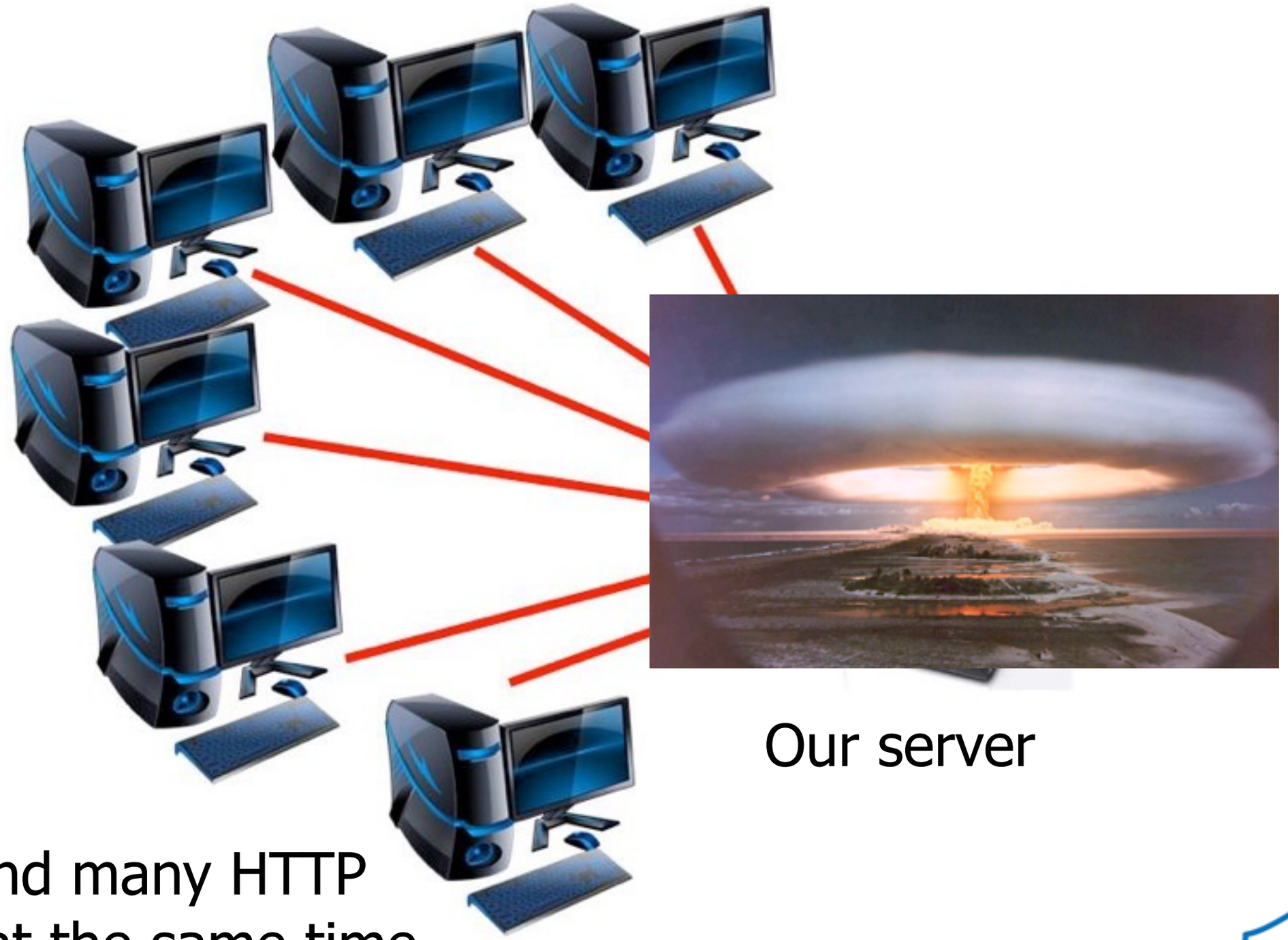
Discussions about web app security

- Lack of security awareness
- A lot of misunderstanding
  - Network firewall can also protect web applications
  - Security is only network security and ISO standard
- Lack of secure coding skills
- Need web application firewall implemented
- Need web application audit

Botnet & DDoS


Bkis
MyDoom DDoS Attack Diagram
Target
Zombie
8 C&C Servers
Master Server from United Kingdom (195.90.1xx.xxx)

Distributed Denial of Service (DDoS) - Flooding



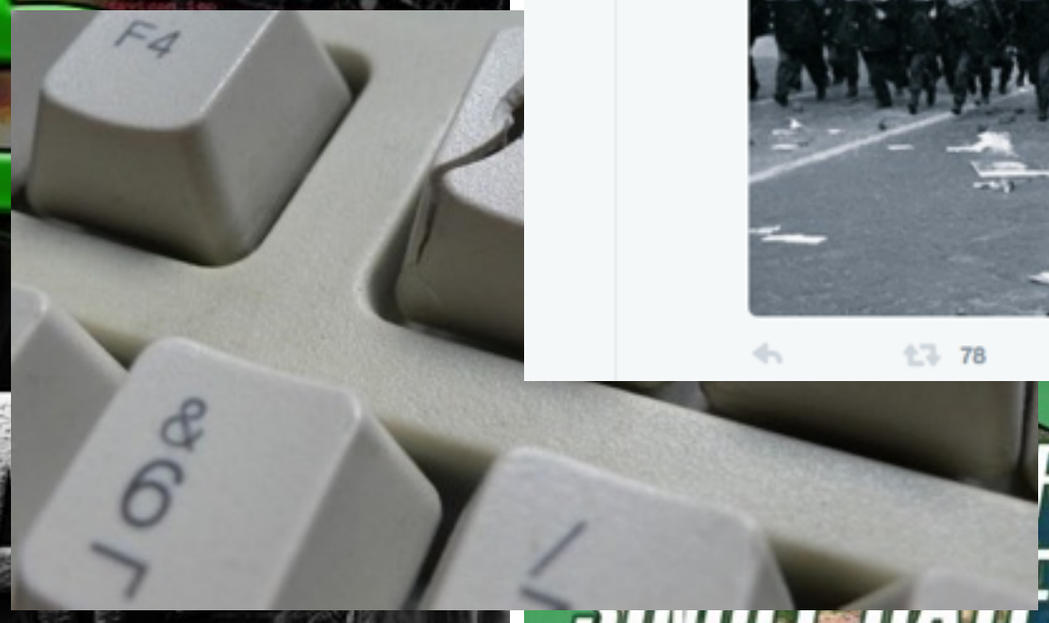
Our server

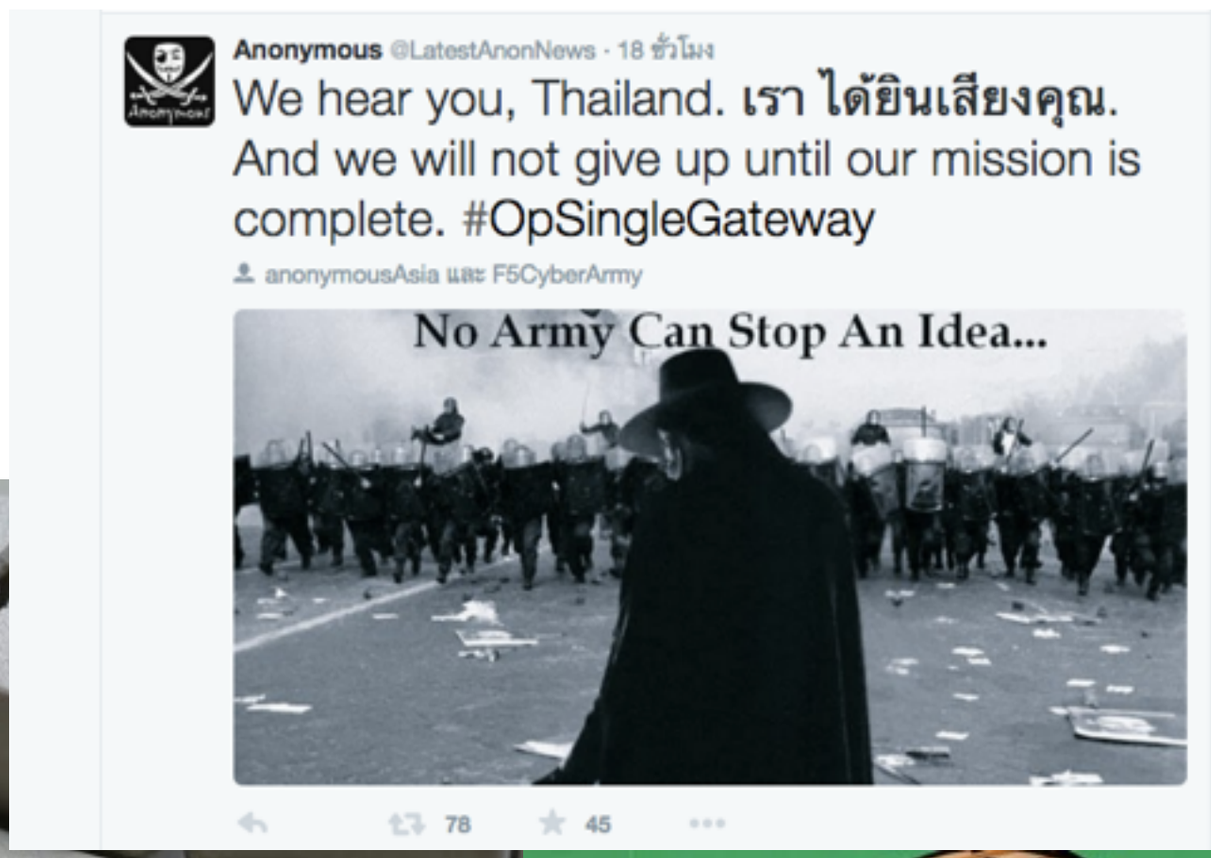
Botnet send many HTTP requests at the same time

Over consuming

Your server is like the donkey, and no, it’s not the donkey’s fault.

Hello Single Gateway !!!!!!!!



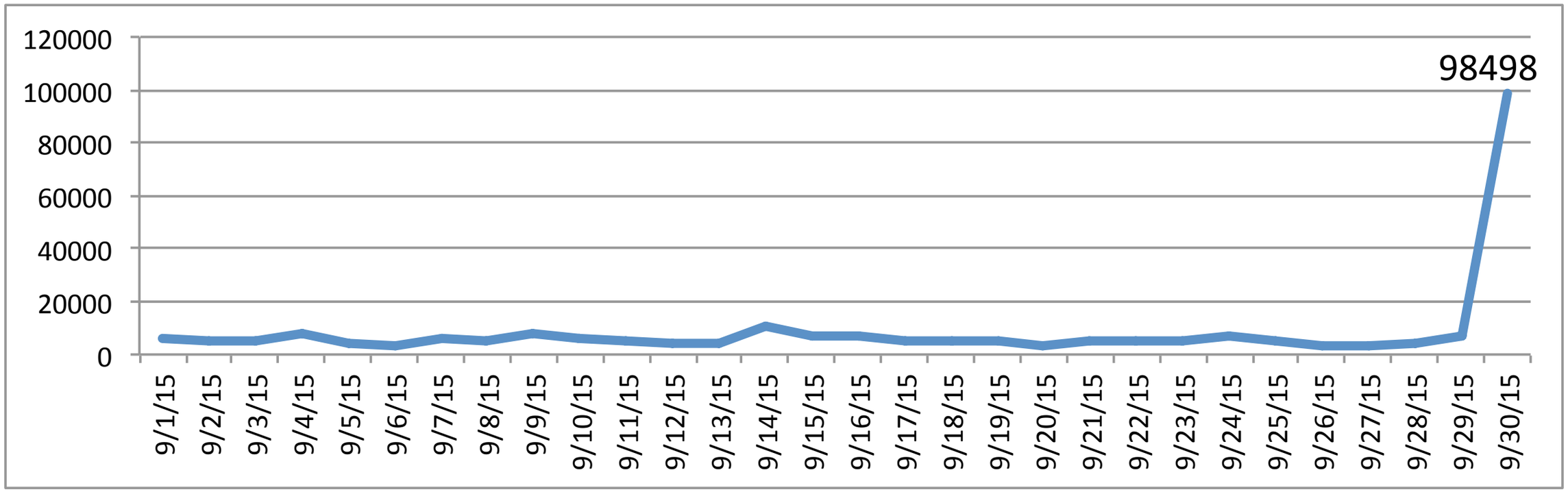


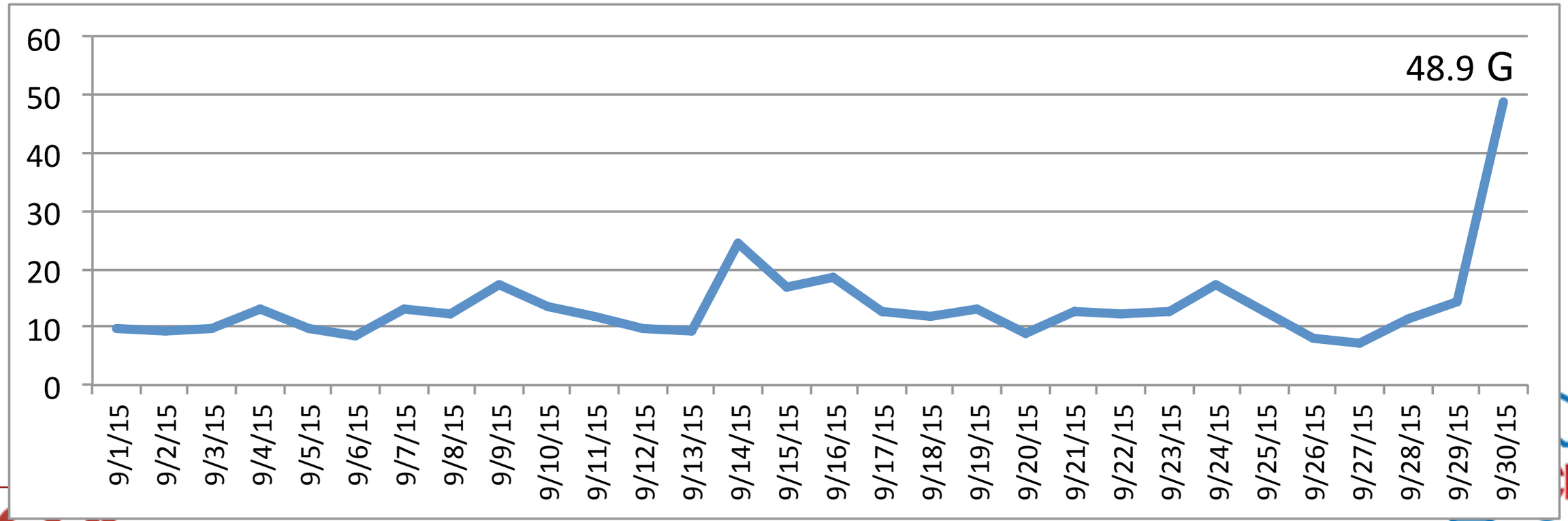
EGA
e-Government Agency

Investigation

- MICT website is running on G-Cloud
- Protections on G-Cloud
  - Next generation firewall
  - Web Application firewall
  - Reverse proxy
- Website is developed by using PHP
  - performance issue
- We found almost 100,000 Unique IPs requested
- This requests consume 48.9 GBytes

Unique IPs and G-Byte consuming





EGA
e-Government Agency

CRT by EGA

Impacts

LOG IN SIGN UP WEB SEARCH

MENU Bangkok Post NEWS

NEWS HOMEPAGE | MOST RECENT | TOP STORIES | POLITICS | CRIME | GENERAL | ASEAN

NEWS > GENERAL

ICT website down ahead planned attack

30 Sep 2015 at 21:30 5,398 viewed 5 comments

WRITER: ONLINE REPORTERS

telecomasia.net

BLOGS RSS

Don Sambandaraksa

Thai govt website DDoSed as CAT customer data leaked

October 26, 2015

Share G+1 4 Like 21 Tweet 22 share Print Email

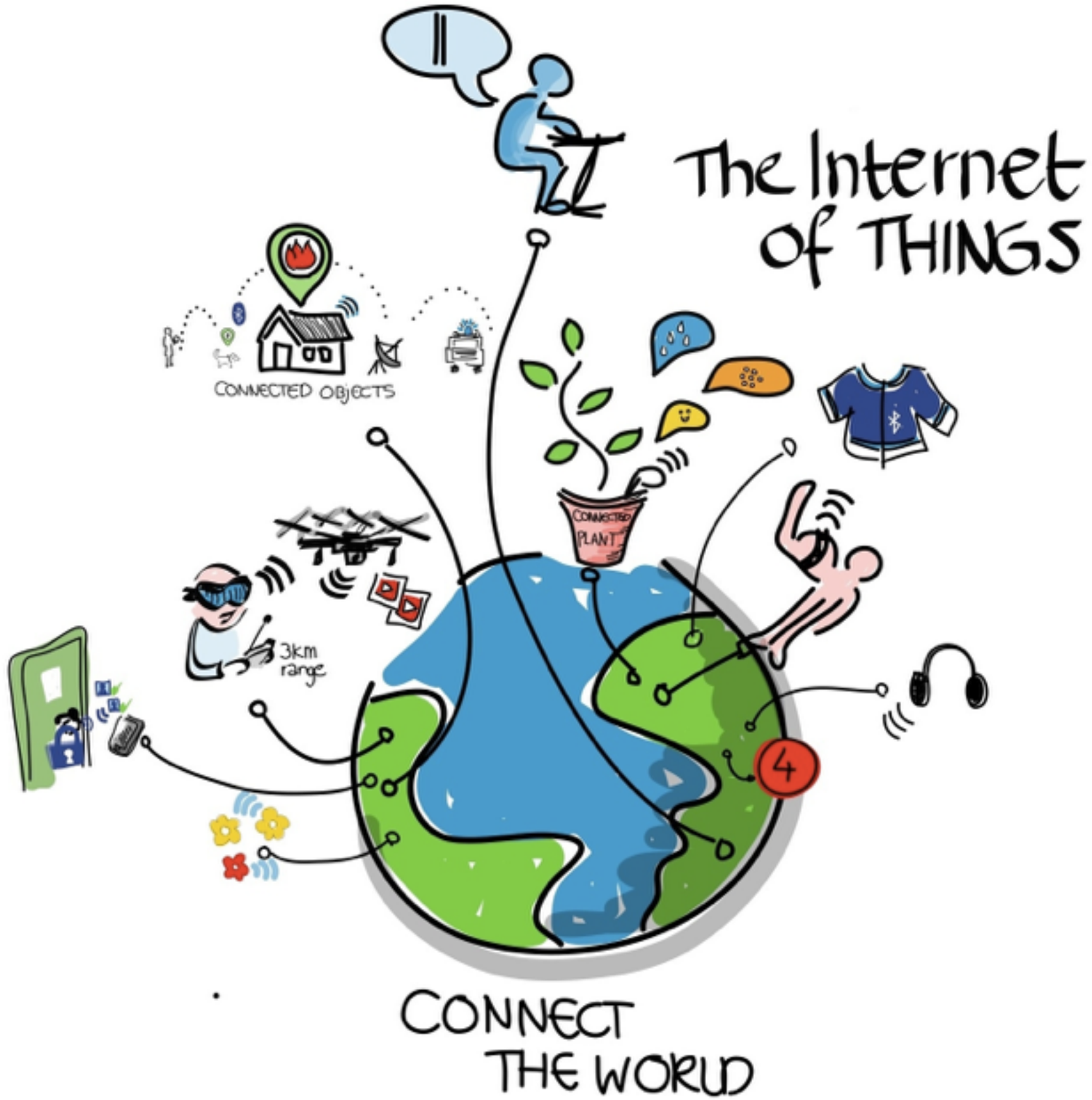
Faced with a wave of DDoS attacks, a horde of hackers claiming to be Anonymous and major data leaks from state-owned CAT Telecom all in protest of Thailand's Single Gateway surveillance program, ICT Minister Uttama Savanayana took to Twitter to reassure people that everything was in order and that we had nothing to fear because we have regular data backups.

EGA e-Government Agency

G-CERT by EGA

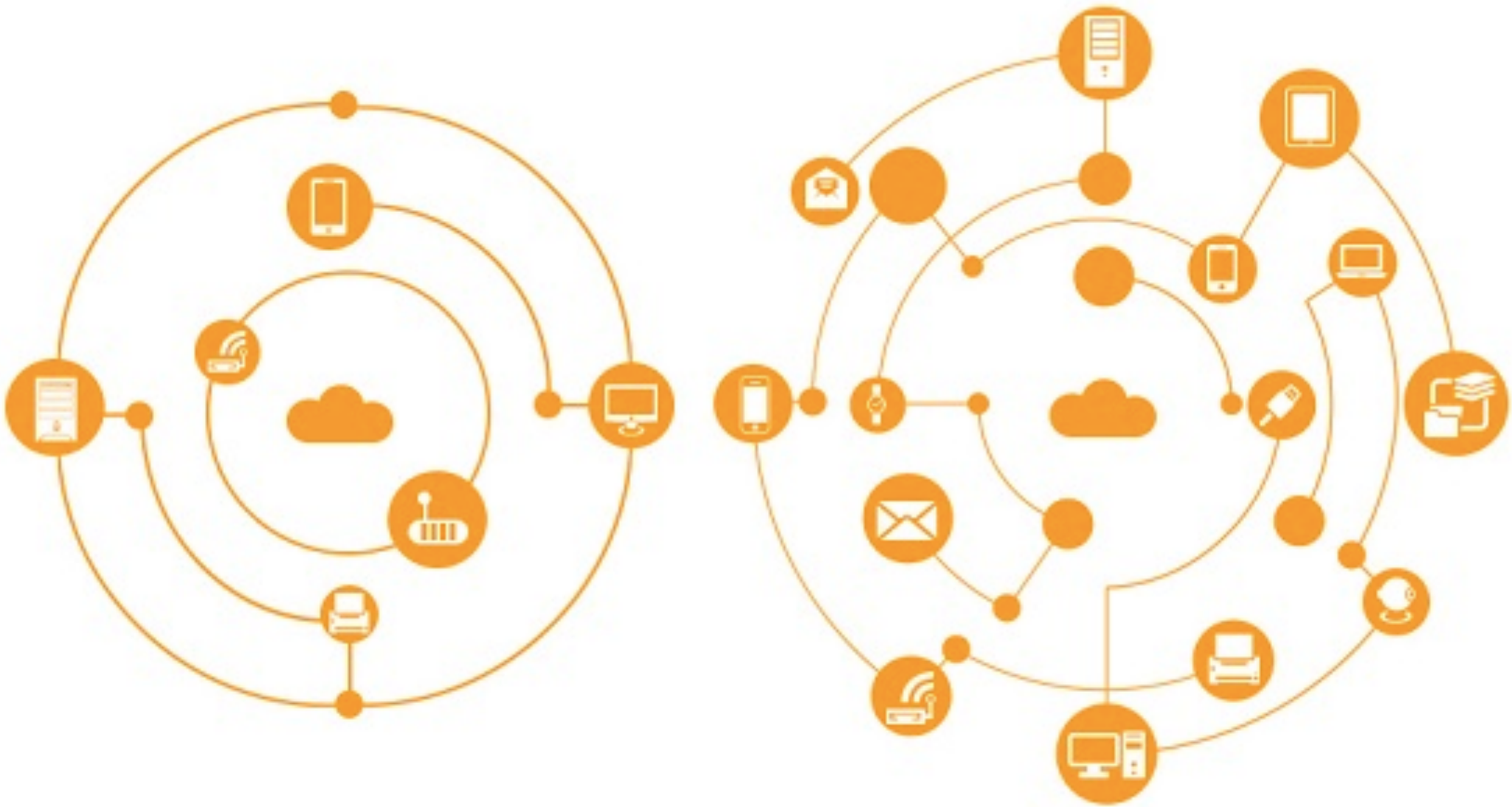
Security benefits on G-Cloud

- Firewall (Next-gen firewall/Application firewall)
- SSL-VPN for Cloud Management
- Two factors Authentication
- Vulnerability Assessment
- ISO/IEC 27001:2013 implementation
- IPv6 installed
- Security monitoring
- Security training courses for customers



http://static.myce.com/images_posts/2015/11/Internet_of_Things.jpg

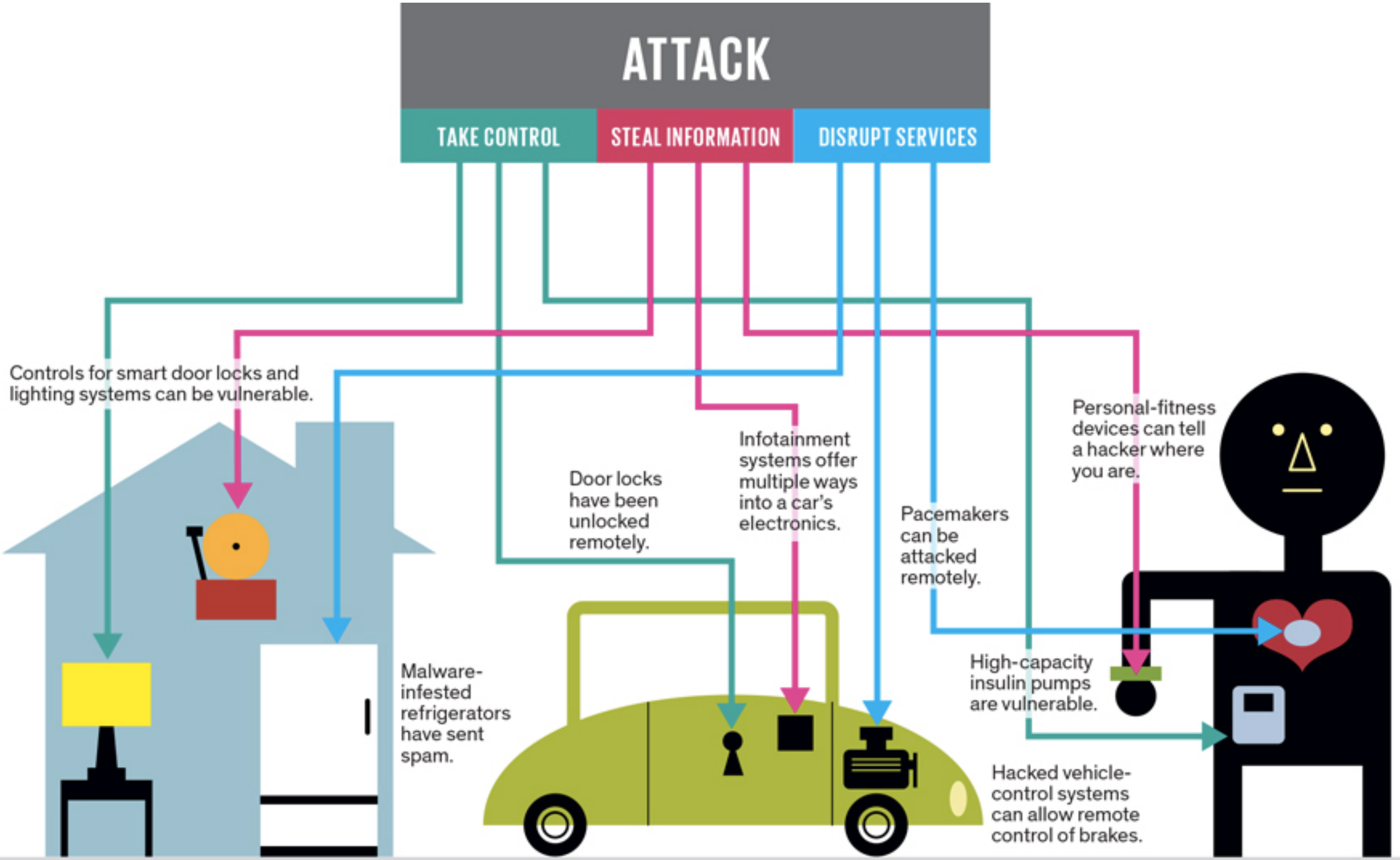
IoT era



Corporate networks then

Corporate networks now

http://blog.trendmicro.com/trendlabs-security-intelligence/organizational-challenges-in-the-internet-of-things/


ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Personal-fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

7 Enterprise risk need to consider

- Disruption and denial-of-service attacks
- Understanding the complexity of vulnerabilities
- IoT vulnerability management
- Identifying, implementing security controls
- Fulfilling the need for security analytics capabilities
- Modular hardware and software components
- Rapid demand in bandwidth requirement

Incident Handling

Overview - Typical IT Security

But.....


More Security Doesn't Make You More Secure
Better Management Does.

Controls will be bypassed

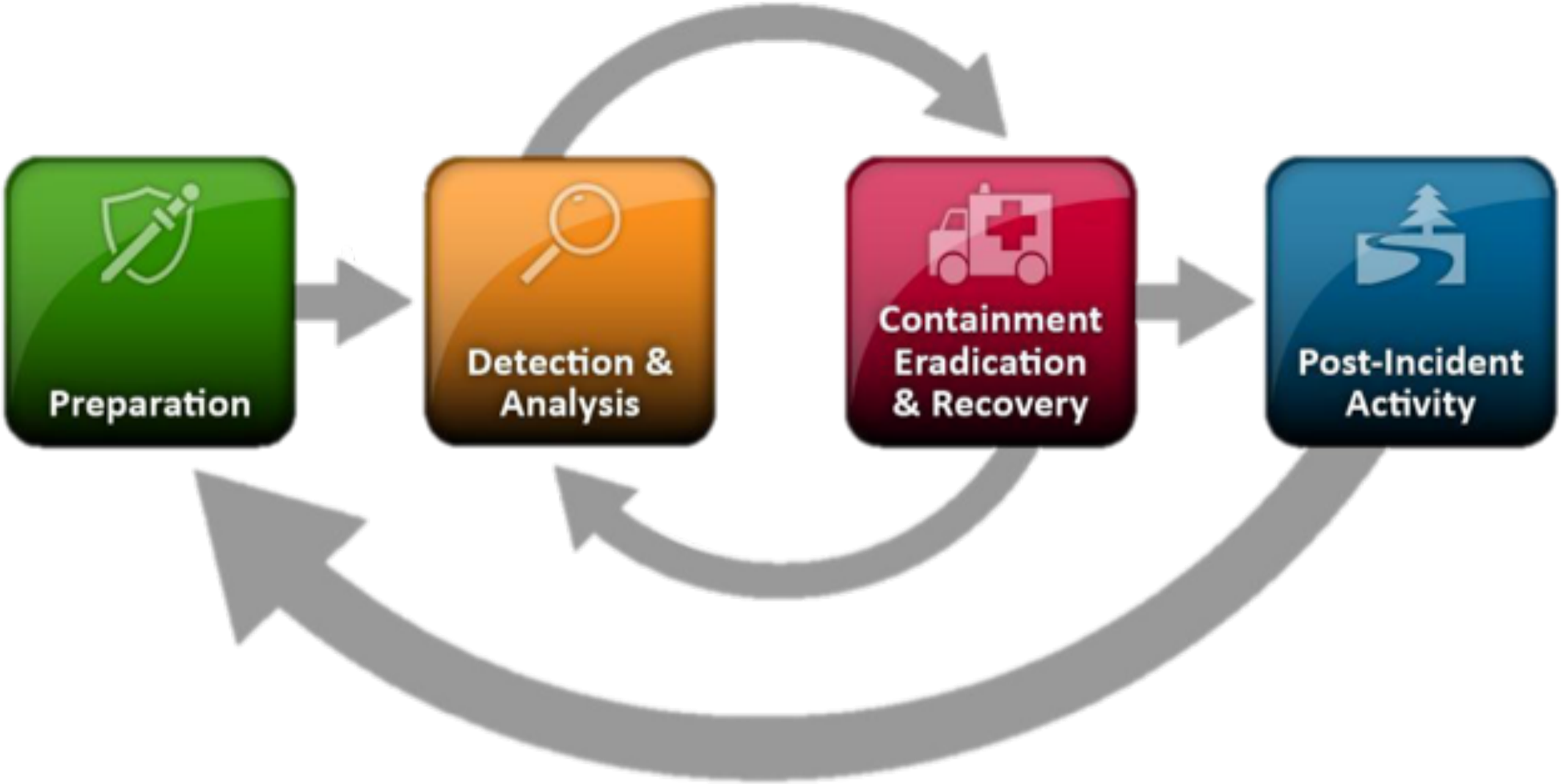
Traditional Incident Response

- Adhoc & Unplanned
- Deal with it as it happens
- Prolonged Recovery Times
- Damage to Company
- Lack of Metrics
- Legal Issues
- Bad Guys/Gals Getting Away

You In Line of Fire

Processes

- Incident Response plan



IR Plan - Preparation

- Build the secured infrastructure
- Security policy
- Setup the monitoring system
- Prepare IR Team and process

IR Plan - Detect & Analysis

- Setup the monitoring system
- Read logs
- Maybe someone reports
- Analysis when something's happened

IR Plan - Response, Eradication and Recovery

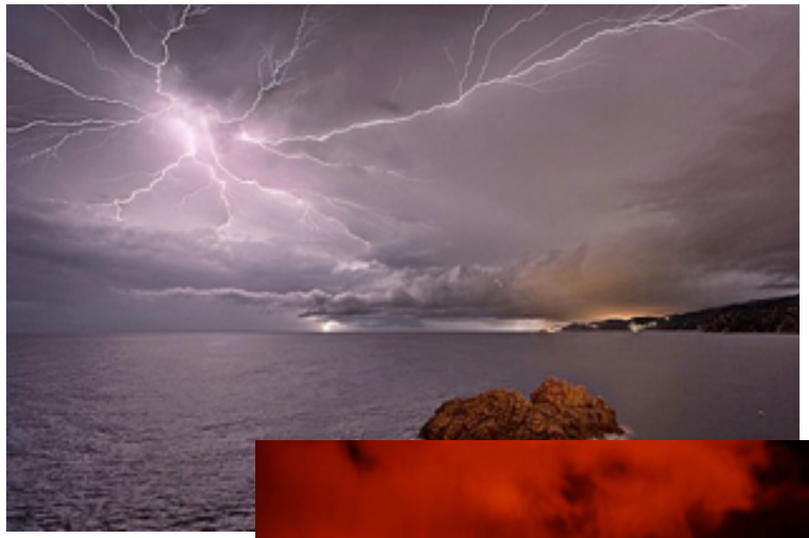
- Find the attackers and how
- Remove or correct the system
- Operate the system again

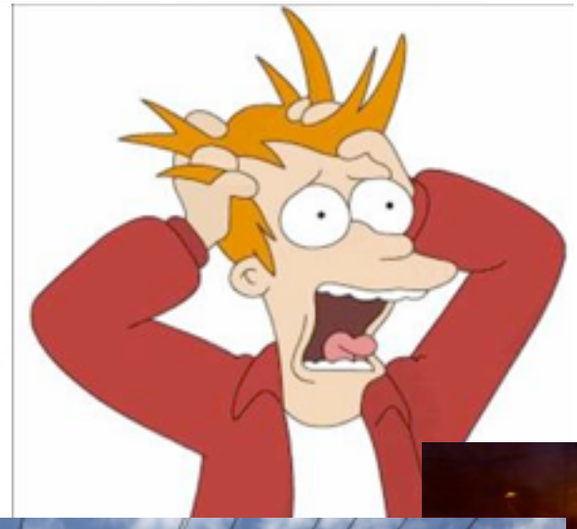
IR Plan - Post incident activities

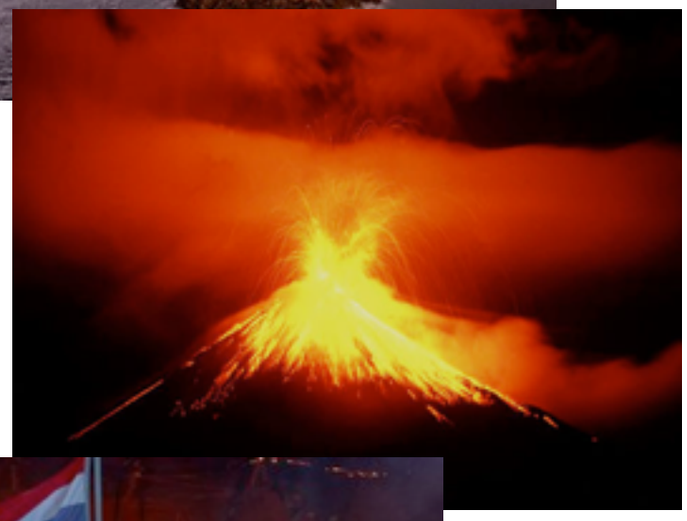
- Study from the attacks
- Prepare the protections
- Keep record

Physical Security

Physical threats







EGA
e-Government Agency

G-CERT by EGA

Why don’t people think about Physical Security?

- Don’t think it’s a threat
- Impossible to secure
- Not enough resources or knowledge
- Haven’t got around to it

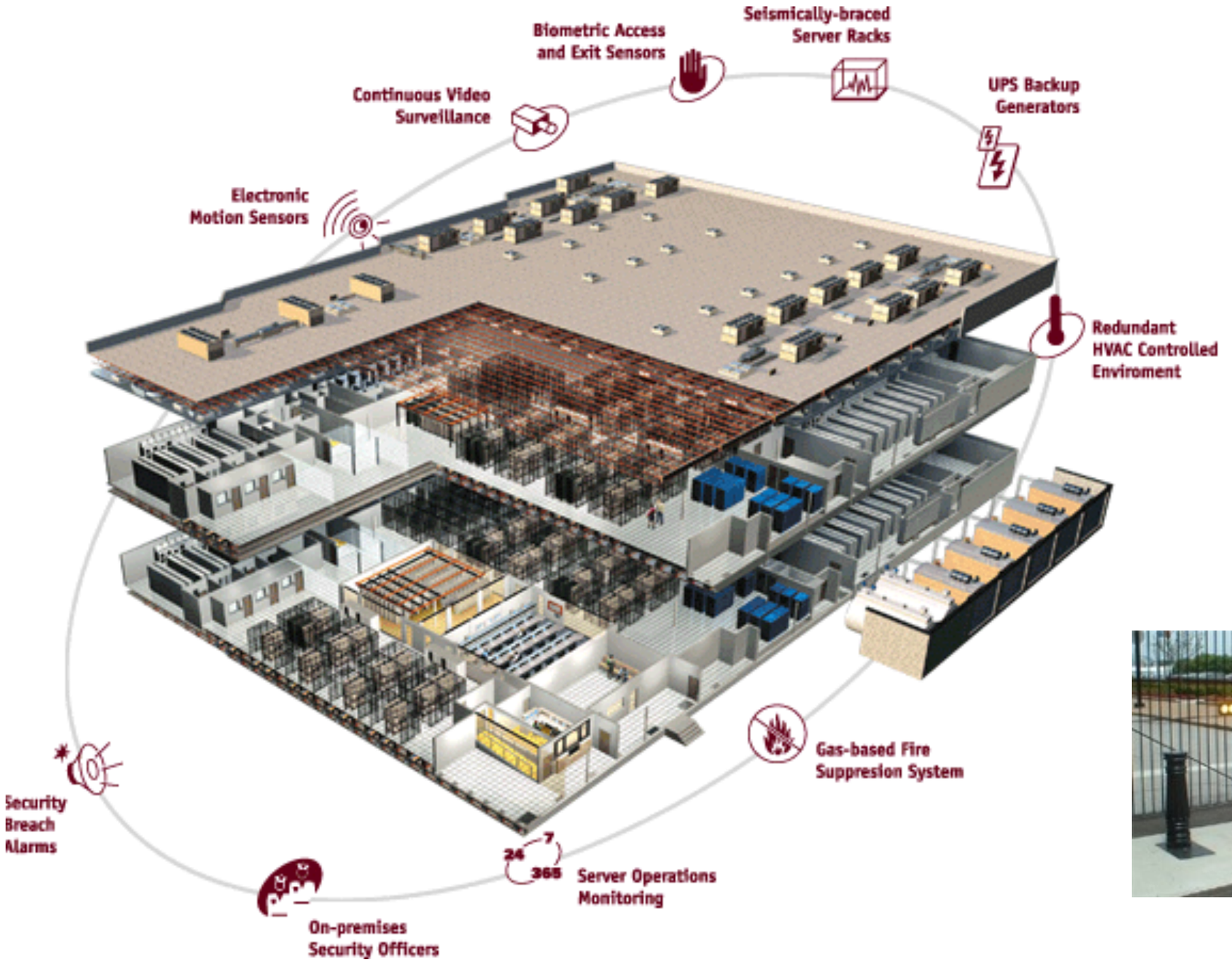
Espionage

- Frequently use physical attacks
- Over 100 billion annually in cost
- Large attacks can be “game over”
- Social Engineering w/ minimal physical attacks have accomplished most large attacks

Social Engineering and Information Gathering

- Social Engineering
  - Co-worker
  - Salesman
  - Interviews
  - Reference checks
  - Impersonation
- Information Gathering
  - Interviews
  - Prospective clients
  - Public tours
  - Dumpster diving
  - Off-site observation
  - Internet

Defence in Depth



Source: Global Crossing website

Physical Security Controls

- Administrative controls
  - Facility location, construction, and management.
  - Physical security risks, threats, and countermeasures.
- Technical controls
  - Authenticating individuals and intrusion detection.
  - Electrical issues and countermeasures.
  - Fire prevention, detection, and suppression.
- Physical controls
  - Perimeter & Building Grounds.
  - Building Entry Point.
  - Box-within a box Floor Plan.
  - Data Centers or Server Room Security.

Focus today

Technical Controls – Entrance Protection

- Entry access control systems
- Turnstiles
  - Revolving doors that can be activated to "lock" and not allow unauthorized individuals to enter or leave facility
  - To prevent "piggybacking".

- Mantraps
  - Routing people through two stationary doorways
- Fail-safe
  - Door defaults to being unlocked.
- Fail-secure
  - Door defaults to being locked.

Technical Controls

- Entry access control systems – Locks
- Mechanical locks:
  - Key
  - Combination locks
  - Magnetic locks
- Electronic locks:
  - Combination lock
  - Proximity / RFID badge
  - Bio-metric

Technical Controls

- Intrusion detection & surveillance systems
- IDS: Sensors that detect access into a controlled area:
  - Photoelectric
  - Ultrasonic
  - Microwave
  - Passive infrared
  - Pressure sensitive

Intrusion Detection & Surveillance Systems

- Closed-circuit television (CCTV)
  - Detect the presence of an object.
  - Recognition of object type.
  - Identification of object details.

Surveillance Systems

- CCTV camera considerations
  - Charge-coupled device (CCD) converts pixels into data signals
  - Cathode ray tube (CRT) converts picture image into data signals
  - Field-of-view is the area that can be captured by the camera lens.
  - Depth-of-field is the area between the nearest and farthest points that appear to be in focus.
  - Monochrome or color camera.

Electrical Power Supply

- Risks to electrical power supply:
  - Blackout: complete loss of commercial power
  - Fault: momentary power outage
  - Brownout: an intentional reduction of voltage by a power company.
  - Sag/dip: a short period of low voltage
  - Surge: a sudden rise in voltage in the power supply.
  - In-rush current: the initial surge of current required by a load before it reaches normal operation.
  - Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power

Electrical Power Supply

- Counter measures to electrical power supply risks:
  - Uninterruptible power supply (UPS) (include transfer switch, battery, transformer, generator, circuit switch, and power distribution unit (PDU))
    - For blackout and fault
  - Surge protector, circuit breaker, transformer, and UPS
    - For brownout, sag/dip, surge, in-rush current, and transient

Electrostatic Discharge

- Risk of electrostatic discharge:
  - A type of electrical surge can occur when two non-conducting materials rub together, causing electrons to transfer from one material to another.
- Countermeasures: Anti-electrostatic discharge (ESD) standards
  - Grounding of equipment to a common point ground.
  - Grounding of personnel: wrist strap, flooring, clothing and footwear.
  - Protected area: Flooring, seating, ionization of air, and humidity control.
  - Marking of equipment, package and facility.
  - Example: Data center: grounding of rack & floors to a common ground, raised floor tiles have conductive gold leafs to support frame to dissipate ESD.

Heating, Ventilating and Air Conditioning (HVAC)

- Types of HVAC systems:
  - Up-flow (forced air above the floor) vs. down-flow (forced air below the raised floor).
  - Water or Glycol.
- HVAC considerations:
  - Air volume cubic feet per minute (CFM) per ton.
  - Humidity control (RH 45% - 60%).
  - Temperature control (72°F ± 2°F).
  - Air Filters.
  - Positive air pressure.
  - Protected intake vents.
  - Alarms: Leak detection, loss of power, temperature, humidity, fire, smoke detector.

Water Supply System

- For cooling, plumbing, sewage, and fire-suppression (outside of server room).
- Water source.
- Water usage.
  - Volume of water.
  - Water filtration.
  - Environmental impact.
- Water pump to maintain pressure.

Types of Fire

Fire Class	Type of Fire	Elements of Fire	Suppression Method
Class A	Common Combustibles	Ashes, paper, wood, cloth, etc.	Water, Soda acid
Class B	Liquid	Barrels of oils, Petroleum, tars, solvents, alcohol, gases	Halon, CO_2, FM-200
Class C	Electrical	Circuits, electrical equipment, and wires	Halon, CO_2 , or Non-conductive extinguishing agent – FM-200
Class D	Dry Chemical	Combustible metals, and chemical	Dry Powder, Halon
Class K	Commercial Kitchen	Food, Grease	Wet Chemicals - Foam

Fire Suppression Systems

- Halon
  - Used so that equipment is not damaged by water.
- FM-200
  - Replacement for Halon without ozone depleting chemicals.
  - It uses chemicals instead of water.
- Carbon Dioxide
  - Does not leave reside after use, does not cause damage to sensitive devices.
  - Can suffocate people.
- Dry Chemicals
  - Not effective against electrical fires.

Types of systems

- Wet pipe
- Dry pipe
- Deluge system
- Pre-Action
- Foam water sprinkler
- Water spray
- Water mist systems

https://en.wikipedia.org/wiki/Fire_sprinkler_system

Fire/ Smoke Detection

- Ionization-type smoke detector detect charged particles in smoke.

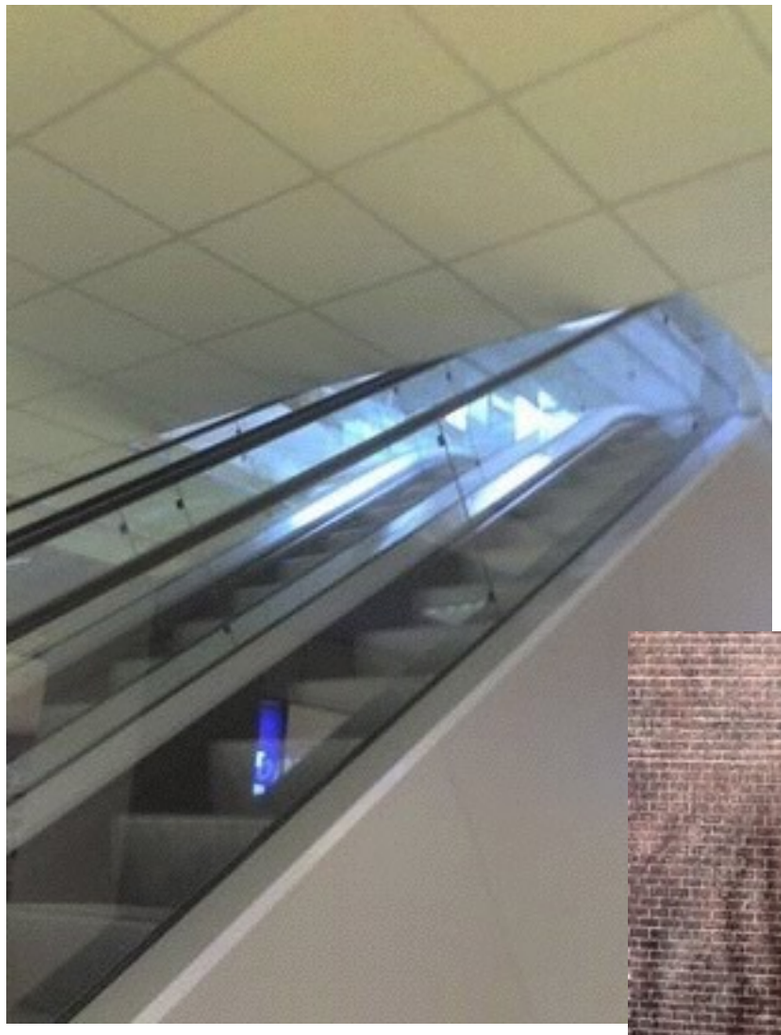
- Optical (photoelectric) smoke detectors react to light blockage because of smoke

- Fixed or rate-of-rise temperature sensor.

Examples of Design Failure

Surveillance

More Examples of Design Failure



Thank you