Cyber Security

Knowledge and Suitable Tools
should be part of a Powerful, Smart Defense System

Mircea Chirita
Expert Asociat la ISEE

Cyber Security

Definition (Wikipedia)

- **Cybersecurity**: is information security as applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet.
- **Computer crime, or Cybercrime,**
  refers to any crime that involves a computer & network
- **Netcrime**
  is criminal exploitation of the Internet.

Computer crime

Classification (Wikipedia)

- Fraud & Financial Crimes
- Drug trafficking
- Cyber terrorism
- Cyber warfare
- Harassment
- Obscene or offensive content
- Threats

Cybercrime

Classification (cont)

FBI

high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud

Interpol

- Attacks against computer hardware and software (exemple: botnets, malware and network intrusion,etc.);
- Financial crimes, such as online fraud, penetration of online financial services and phishing;
- Abuse

Cybercrime

Meaning to Commercial Companies

Where are targeting the cyber criminals?

Cybercrime can endanger governmental institutions, private organizations and individuals alike.

The attack vectors are materialized into :

- Stolen financial resources
- Information loss or theft / Knowledge/ Secrets /Trade Advantages /Tangible & Intangible (Intellectual Capital Assets, Intellectual Property & Personally Identifiable Information - PII)
- Financial resources required to fix business disruption, equipment damage, collateral damages, claims, etc.
- Revenue loss, reputational damage.
- Etc.

Cyber Security

Status

McAfee sponsored report.... June 2014

- "Cyber crime costs global economy $445 billion a year! (estimates of the annual damage)

KPMG Report.... Aug. 2014

- revealed > 96% organizations experienced a significant IT security incident in 2013
- majority of IT organizations are aware that some of their security measures are immature or ineffective
- only 33 percent have high confidence in the likelihood that their organizations will improve their less mature security controls.

Cyber Security

Company Issues

Objective Problems

KPMG Study Sweden 2014 identified that traditional defense become almost ineffective for today's malware.

- 43 security incidents/day => average of 2 infected hosts/day
- 93% of the organizations were breached
- 79% were "data exfiltration"
- 49% of the detected malware was unknown
- 52% of identified malware were unknown to AV
- 83% of the callbacks were related to data exfiltration (sensitive info!!)
- Increase of Multi-Vector, MultiStage Attacks Type APT Attacks
- Increase of Multi-flow 'Watering Hole' Type APT Attacks
- New type attack class is emerging (System Hopping Malware...)

Cybercrime

Cybercrime Economy

New Realities:

- **Nasdaq** - Data Leak (NDAQ Oct 2010) - Detected by FBI
- **RSA** - Security Breach (March 1, 2011) with large implications for other security measures and tools;
- **JP Morgan** - Massive bank hack (summer 2014, >90 servers Affected and >83m account holders);
- **Home Depot** investigating 'massive' hack (compromised 56 million payment cards)
- **Target** investigating 'massive' hack (40m Stolen Credit Card Numbers: How Target Blew It)
- 1.2 billion Internet credentials stolen by A Russian crime ring CyberVor
- 5 million Gmail passwords leaked
- Four teenage hackers breaking into the systems of the US Army and Microsoft (to steal over $100 million in intellectual property)

Cyber Security

Cybercrime Economy

Lesson learned?
Do we prefer to think we’re not a target?.. Are we?

- Break-ins are faster then ever, everyday more sophisticated
- Successful attack rate is continuously increasing.. are we ready?
- Although failed, Target had a large security team, state-of-the-art security tools, available IR plan & team
- Data breach preparedness is a 'live system', a team sport, not a 'compliance exercise';
- Do we rely on 'operational tools', proper standard & framework implementation, Are yours measure ready?
- Is yours business ready for a data breachable? Is it ready to react?
- Many time the evidence of an attacks is in front of us ...
- Are we prepared to improve attitude?   .. preparedness?
- A new Mindset is a 'must have' !

Cyber Security

Company Issues

The impact of being not aware:

KM-Trends 2013: Attack the Security Gap

- 243 days to discover
- 69% organizations learn from an external source

Undetected Presence (**KPMG Report**)

- 229 days – Average presence on victim's system.
- 2 287 days longest presence (14 less then 2012)

Last major succesful attack

- **JP Morgan** : undiscovered 2 month attack
- "**Home Depot" Retailer** US/Canada: cca 5month 'massive hack 56 mil. Payment cards compromised'..'estimated costs of $62 mil..' specific crafted attacks tools (hadn't been previously used);
- "**Target Retailer**" US/Canada: cca 20 days 'massive hack 40 mil. payment cards compromised'..'incurred costs of >$200 mil.' ("Backoff" malware attack tool)

Cyber Security

Company Issues (Cont)

The impact of being not aware: (cont)

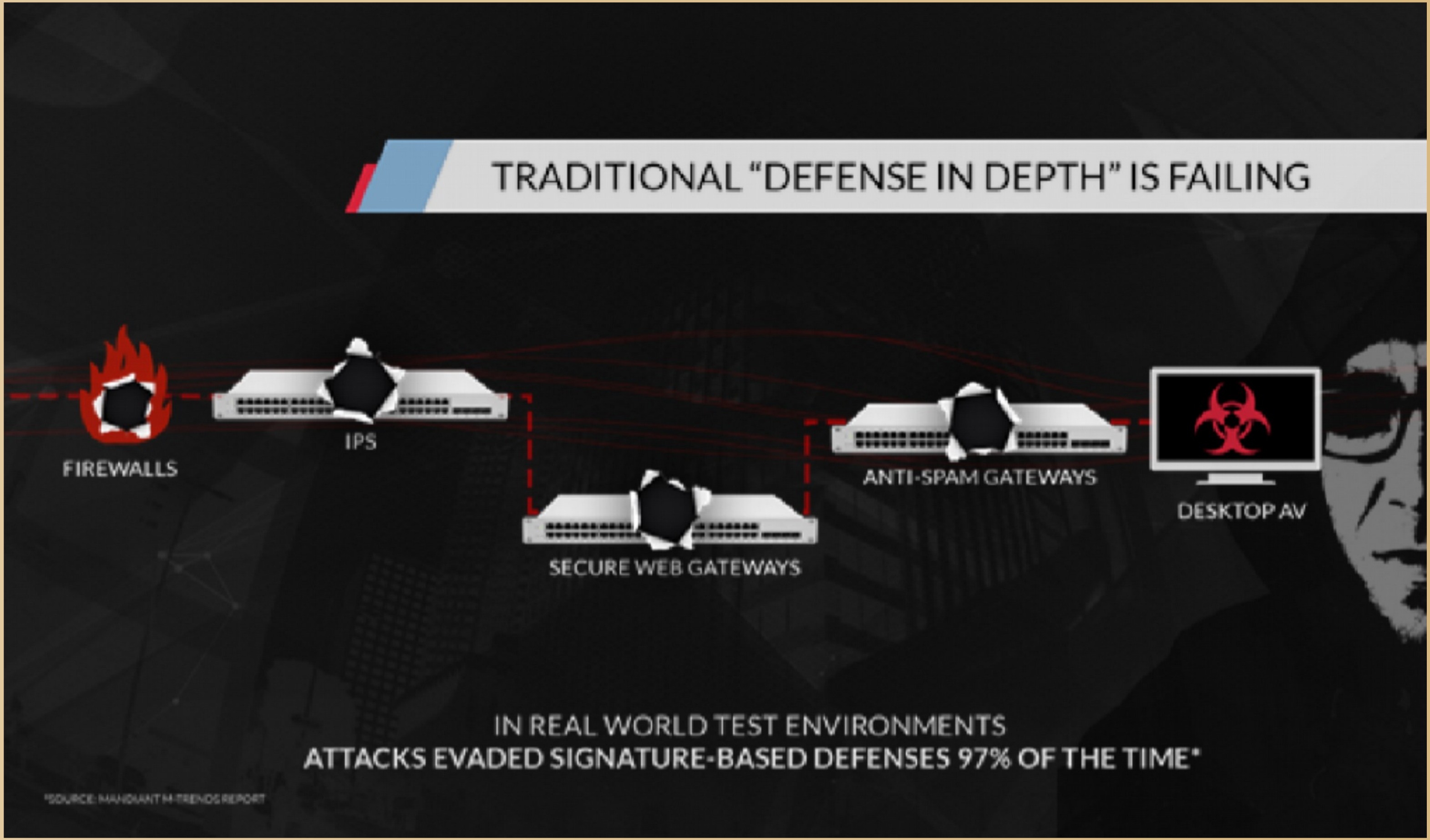
Gartner research note Feb 2014

- Most enterprises are ‘overly dependent’ on blocking & prevention firewalls, anti-virus which are ‘decreasingly effective’
- Advised "to take a more *pro-active* rather than *reactive* approach
- Assume that their systems are under a state of constant compromise that requires *continuous monitoring and remediation*
- Put greater resources & investment into building out
  - threat detection, response and predictive capabilities.

Cyber Security

Compulsory Requirement for Change

ISEE
Extreme Events Think-Tank



TRADITIONAL "DEFENSE IN DEPTH" IS FAILING

IN REAL WORLD TEST ENVIRONMENTS
ATTACKS EVADED SIGNATURE-BASED DEFENSES 97% OF THE TIME*

*SOURCE: MANDIANT M-TRENDS REPORT

Cyber Security

Is Cybersecurity Actually Broken?

- Recent (known) retail breached entities,
- KPMG Report,
- Gartner Report,
- CIO Report,
- RSA case,
- etc.

are validating the weaknesses of our current cybersecurity methodologies and solutions

Cyber Security

Compulsory Requirement for Change

Different Type Approach:

Realistic:

- 100% "security status" is not achievable..

Pessimistic:

- *We are NOT winning!*
- *“In 2020, enterprises will be in state of continuous compromise.”* Gartner
- *“There are two kinds of companies: those that have been breached and those that don’t know about it yet”*

CIO Fortune 100 company..

Cyber Security

Building a new security system / Building Preparedness

The process could start from the failure's roots:

- Improper security operational tools (effectiveness to be increased)
- Inappropriate standards and frameworks implementation
- Company Culture - improving company security culture (awareness, training, etc.)
- Authorities: lack of involvement, mismanagement lack of preparation, and suitable strategies,
- Improve security attitude and preparedness
- Etc.

Cyber Security

Compulsory Requirement for Change

ISEE
Extreme Events Think-Tank

Compulsory Counter Measures / Improvement Areas with direct Impact :

- Develop & switch to a new Security Mindset
- Better Standard Framework Implementation
- Adopting a 'Resilient Type Approach'
- Increased effectiveness by advanced cyberforensics
  'Operational' Security Tools
- Deal quick with a new incident (fast, high-performance..)

  “Response is the closest thing we have in IT with ‘dogfighting”’

  Bruce Schneider, Blackhat 2014
- Extension Use of Encryption
- Surface the Intangible
- BBB – Better Ballanced Budget
- IT & Company culture
- Better Awareness / Security Intelligence Sharing & Analisys,
- Etc..

Cyber Security

Company Preparedness

Security and Standard Framework (Information security):

- ISO/IEC 27001-8
- ISO/IEC 24762:2008
- ISO/IEC 27031:2011
- ISO/IEC 27035
- ISO 31000:2009
- ISO/IEC 38500:2008
- BS 7858:2006+A2:2009
- BS 25999-1
- ISO 22301
- BS 25999-2
- BS 25777:2008
- PD 25111:2010
- PD 25666:2010
- NIST SP 800-55
- NIST SP 800-61
- COBIT
- ITIL v.3 (International)
- ISO/IEC 20000
- NFPA 1600
- PAS 200:2011
- PCI DSS v3
- NIST

Cyber Security

Company Preparedness

Security and Standard Framework:

Usual Implemented Standards

- ISO/IEC 27001 (control point based)
- SANS TOP 20 CSC (procedure based)
- PCI DSS (global payment)
- NERC-CIP (Energy Infrastructure)
- ISO 22301 (Business Continuity)

Cyber Security

Company Preparedness

ISO 27001 strengths

- A "would be best choice" for yours main core CyberSecurity system;
- A minimum standard for an effective information security
- Internationally accepted, and a mature one;
- A fast growing international adoption /No.1. Romania 291%
- A “best practices” framework
- Flexibile – 'Control point' based
- Scalable – to be easily adopted by (and fit) small but big organizations as well.

to be in the meantime or later complemented by SANS CSC 20, NERC-CIP, PCI-DSS, NIST, ISO 22301.

Cyber Security

Company Preparedness

Why ISO 27001 Implementation Fails

- In general frameworks and security controls can be misused, underused, or not used at all.
- Poor implementation (many organizations do not fully understand the standard implementation, missing proper consultancy, etc.);
- Formal implementation with few points in common to a real "management system"
- "Checkbox security"= Security ! – an approach that undermines the real Security
- Continuous pressure increase due to the ever compliance increase
- "Permissive" paper-based system implementation that shift its purpose
- Misunderstood that ISO 27001 is a starting point towards security, a benchmark and not the final solution.
- No real correlation process - (approved) specific system & management Documents
- Development of 'Organizational islands' or 'Organizational silos'

Cyber Security

Company Preparedness

ISEE
Extreme Events Think-Tank

ISO/IEC 27001 Why Implementatio Fails

- Too many standards, building employee confusion
- Registrars play both the auditor and implementation consultant role creating hereto a major conflict of interest.
- The minimum acceptable level of control varies between registrars
- Lots of misinformation concerning the level of effort, documentation
- Fail to use an intangible approach and tools specific in identifying and quantifying intangibles.
- Insider Threat: People known as organization’s “greatest assets” are also its greatest threat.
- Missing a "Continuous monitoring” strategy,
- Missing a proper "disaster recovery / business continuity planning

Cyber Security

Security Maturity Framework & Tools

Systemic Implementation Tool Requirements:

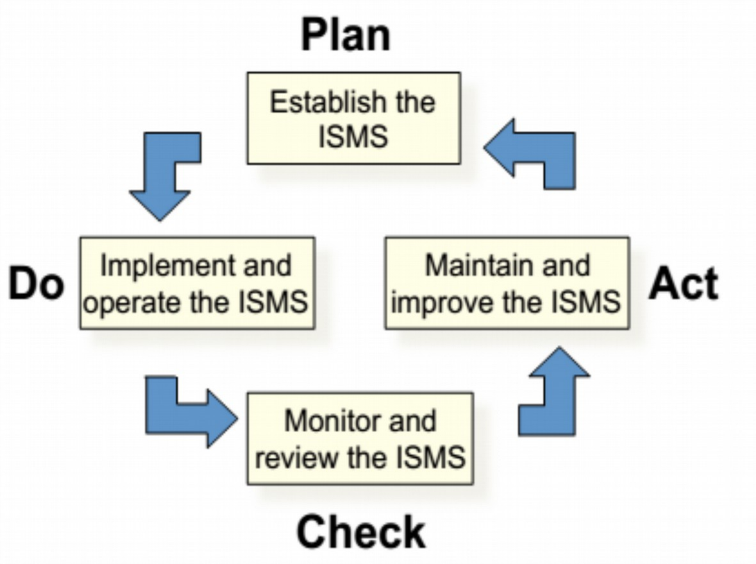
- An useful groupware to diminish 'organizational silos' effect
- Minimize the gaps, allow building bridges between “management layers” & “system islands”
- Better system management improve “system compliance” and its effectiveness
- Easier to improve and implement "continuos monitoring"
- "process implementation" vs "solution"
- Easier to deal with the "human side" (groupware)
- Easier to access and use statistics
- Easier to deal with multiple standards and frameworks
- Easier to deal with system assessment, also self-assessment
- A perfect Complement to a SIEM

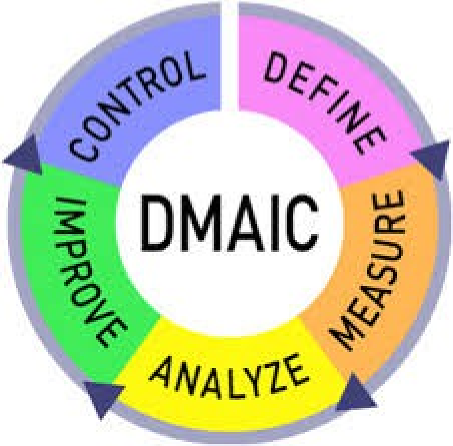
Cyber Security

Security Maturity Framework & Tools

Systemic Implementation Tool (cont)

Enable barely used PDCA/ DMAIC to be 'back on track'


Plan
Establish the ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check



Cyber Security

Thank you!