

# Project FORWARD

*Managing Emerging Threats in ICT Infrastructures*  
*ICT-216331-FORWARD*



## Security Threats in Banking ICT Systems



Assoc.prof. Luben Boyanov  
Assoc.prof. Valentin Kisimov

Nice, France  
May, 2009

**If I am vulnerable - I see threats**

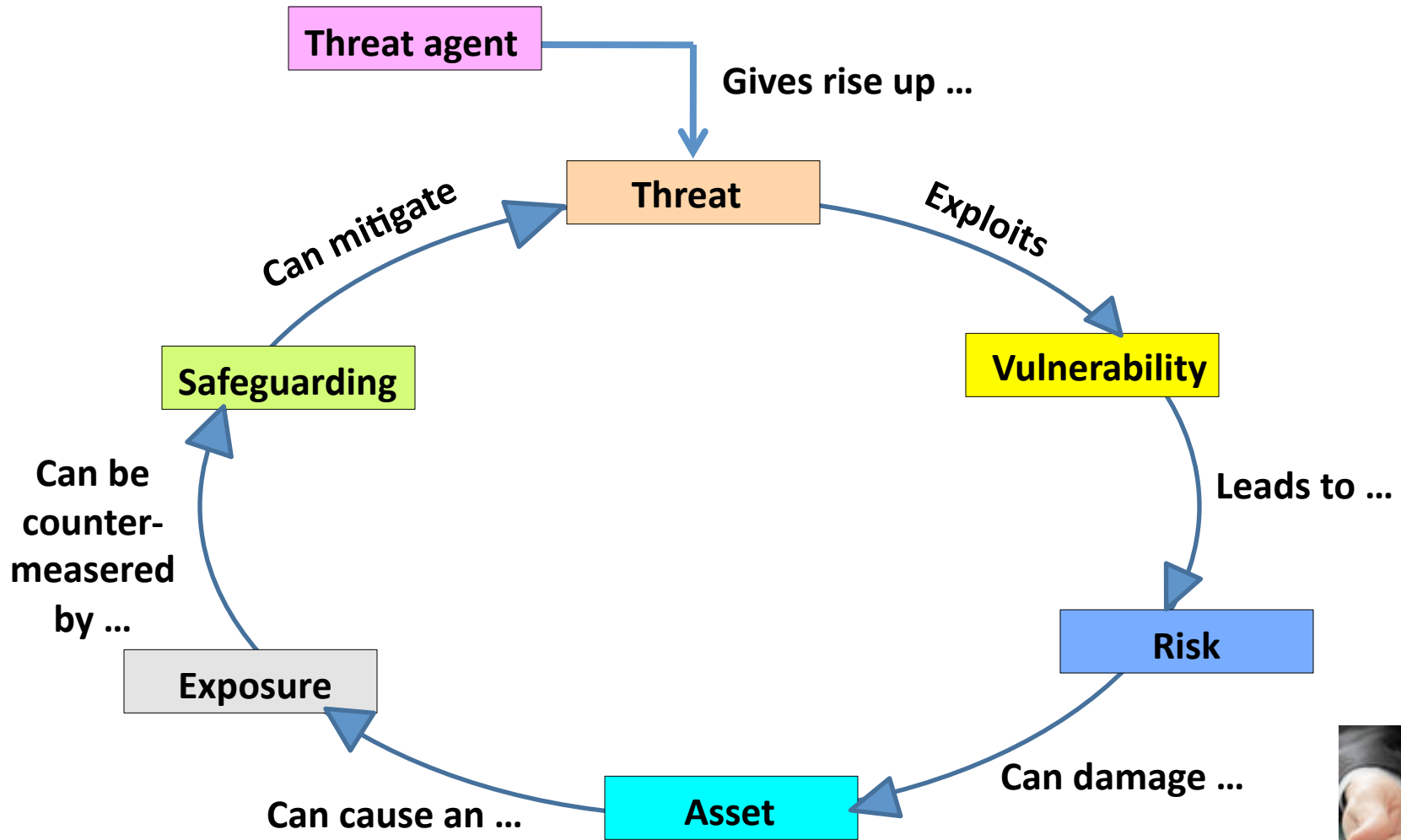
**If am not vulnerable (?) – I expect threats**



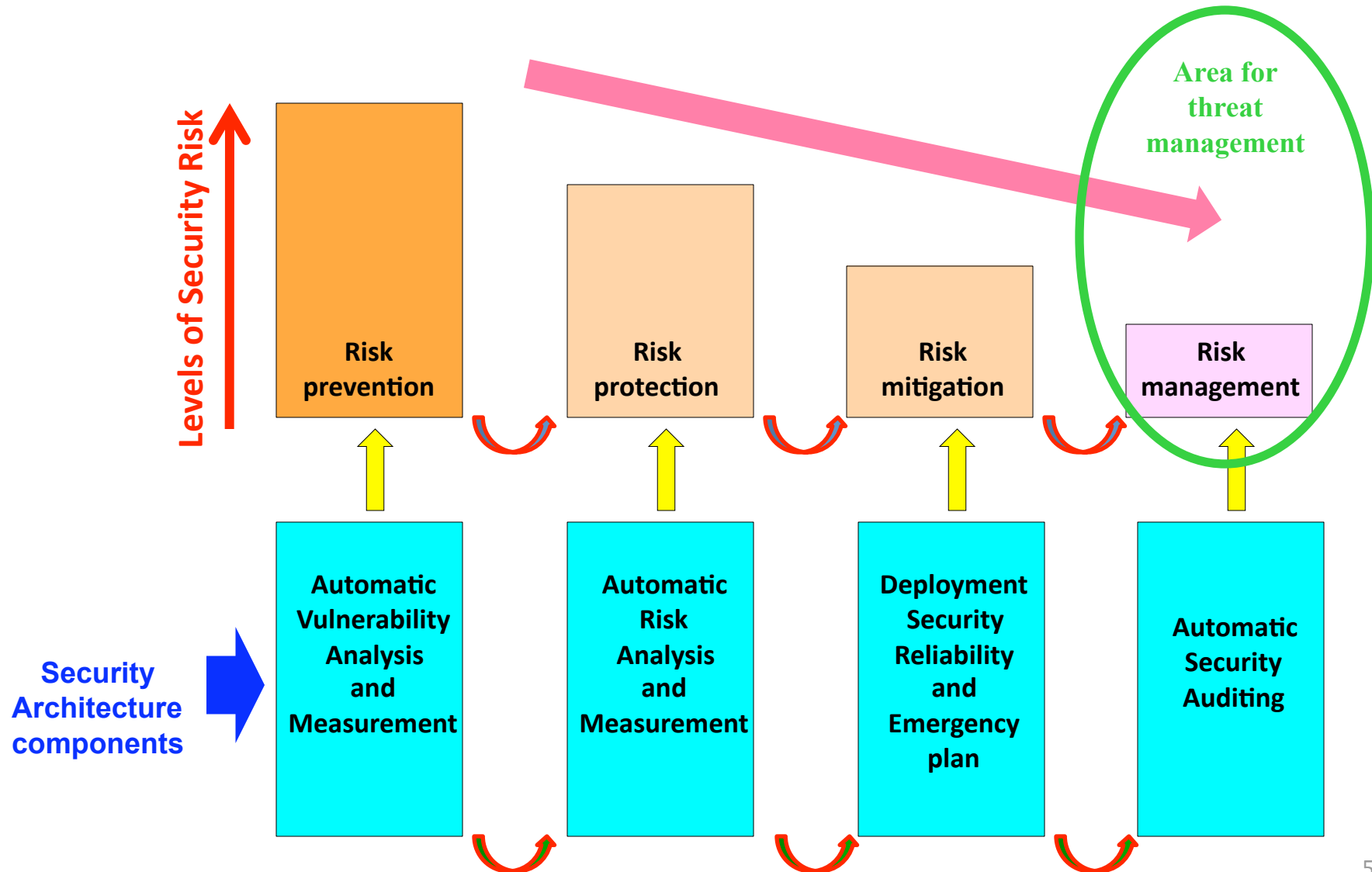
- **Vulnerability** – a weakness that may provide an attacker the open door for unauthorised access and actions
- **Threat** – any potential danger to Information security
- **Threat agent** – an entity taking advantages of the vulnerability
- **Risk** – the likelihood of a threat agent to take advantage of a vulnerability ,causing corresponding business impact



# Threat *action-protection* lifecycle



# Methodology of Risk management, decreasing the effect of the threats



# Threats to customers' computers

- **Phishing**

- Using hoax email claiming to be from the bank

- **Spyware**

- Type of software that covertly collect end-user information while on Internet

- **Adware**

- Type of Spyware, used by marketers to track end-user's habit and interest for the purpose of future advertising

- **Virus**

- Software that affixes itself to another program like word processing and spreadsheet, run if the infected program is running and attempts to reproduce and attack other programs; Normally distributed via email

- **Worm**

- Like Virus, but looking for security holes to install into the computers and replicate

- **Trojan horse**

- Added to a program which does valuable actions, loaded with infected programs or as anti-virus programs



# Errors and Omissions as threats

➤ 65 percent of losses to organisations are results of errors and omissions \*

➤ Threats:

- **Data entry;**
- **Data editing;**
- **Program bugs;**
- **Installation errors**
  - About 10% of the security errors
- **Operation errors;**
- **Remote employees' computers used as "Security bridge";**
- **Back doors in programs:**
  - **Back Orifice** – secondary entrance;
  - **NetBus** – for Windows systems;
  - **Sub7** – secondary entrance without authorisation;



\* Computer System Security and Privacy Advisory Board, *1991 Annual Report (Gaithersburg, MD), March 1992*, p. 18.

# Fraud and Theft

- Internal and external people can do fraud and theft;
- As long as people feel cheated, bored, harassed, endangered, or betrayed at work, sabotage will be used as a direct method of achieving job satisfaction;
- Malicious hackers, called crackers, break into computers without authorisation
- Hackers attempted to break in at least once every other day / multiple per day;
- Mixing private and banking information on laptops;
- Insiders have easy access to banking internal systems;

- Threats:

- Fraud of banking information from employees' laptops** being remote;
- Copying of internal banking files;**
- Copying customer private data;**
- Change customers' private data;**
- Extraction of customers' private data;**
- Deleting data;**
- Holding data hostage;**
- Changing banking data;**
- Destroying hardware or facilities;**
- Planting logic bombs** that destroy programs or data;
- Degradation / disruption of system availability;**
- Password guessing and cracking.**



# Network threats (1 of 2)

- **IP spoofing attacks**

- masquerading trust system in order to get unauthorised access

- **DNS spoofing attack**

- send users to a different location than the official bank web site

- **Man in the middle**

- one of the more complex and sophisticated forms of security breaching approaches

- Applicable of WAN and on LAN

- An agent collect, record and retransmit the data as though nothing is happening

- have increased considerable since the introduction of wireless networking

- **Relay attack**

- variation on the man-in-the-middle

- the transaction data is recorded for the purpose of data modification and it is resent to the server at a later time for nefarious purposes

- **TCP/IP Hijacking**

- similar to man-in-the-middle, the rogue agent sends a reset request to the client so that the client loses contact with the server while the rogue system assumes the role of the legitimate client



# Network threats (2 of 2)

- **Denial of Services (DoS)** attacks

- **Ping flood** – issuing in big sequence *ping* command
- **Smurfing** – like Ping flood with the IP address of the server-victim
- **TCP SYN flood** – sending ACKs to the server accepting the connection
- **Fraggle** – like Smurfing but with UDP
- **Land** – sending fake SYN packet with same source / destination IP addr, confusing the victim
- **Teardrop** – uses weaknesses in TCI/IP implementation stack, by sending messages fragmented into multiple UDP packages, corrupting the offset data in UDP packet
- **Bonk / Boink**– attack of Windows systems, transmitting corrupted UDP packets to different UDP ports

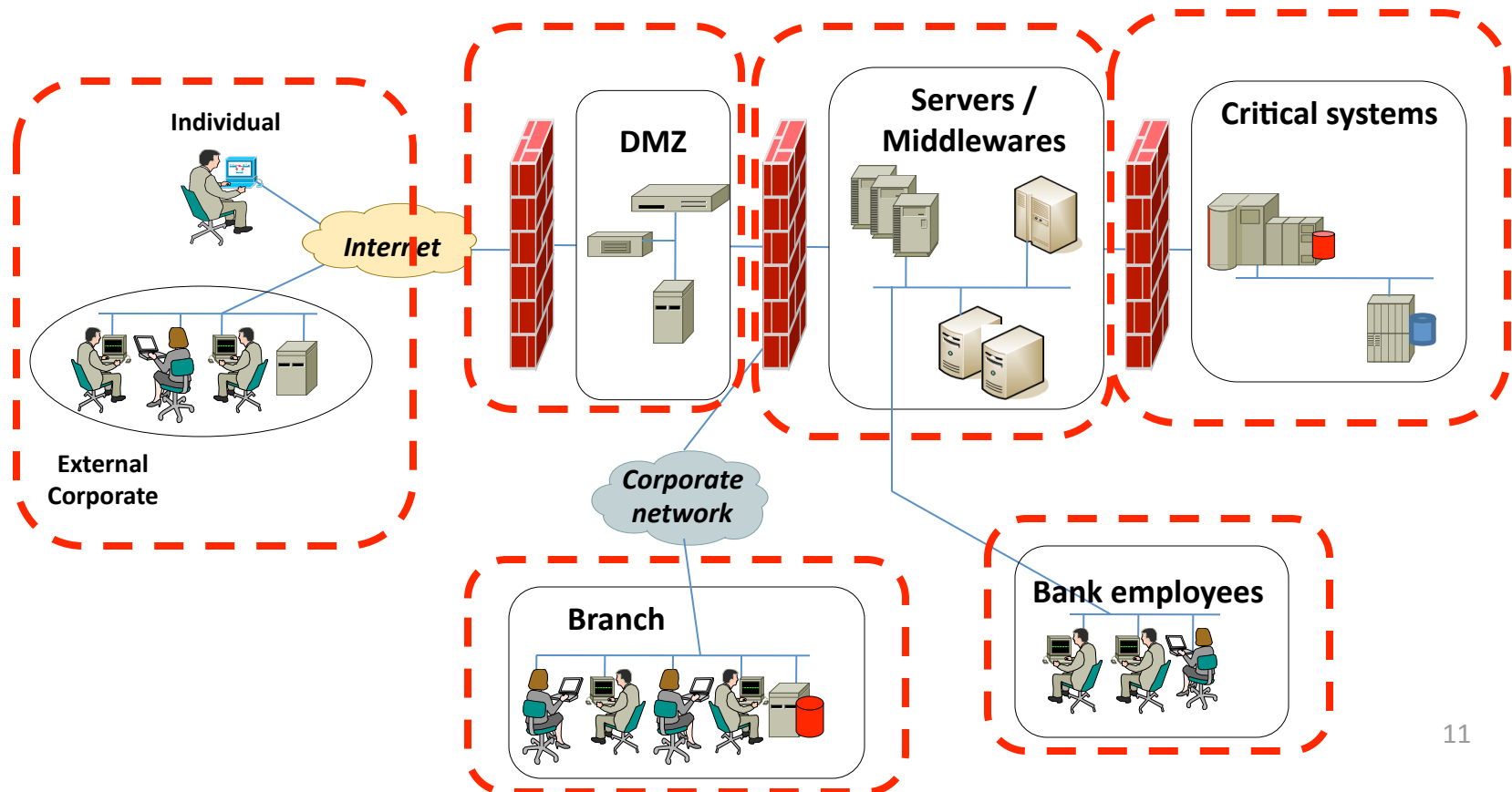
- **Distributed Denial of Services (DDoS)** attacks

- use the same basic attack methodologies as DoS, with the exception that the attacks are initiated from multiple client systems
- the infected systems – zombies, are waiting to be given instruction for attack



# There are 6 Security domains in Banking ICT systems

- Customers
- DMZ
- Branches
- Servers / Middleware systems
- Critical systems
- Internal employees



# Threats in *Customers'* security domain

#	Threat	Prob
1	Phishing	H
2	Spyware	H
3	Adware	H
4	Varus	H
5	Worm	H
6	Trojan horse	H
7	DNS spoofing attack	M
8	Man in the middle	M
9	Relay attack	M
10	TCP/IP Hijacking	M



# Threats in *DMZ* security domain

#	Threat	Prob
1	Program bugs	M
2	Back doors - Back Orifice	M
3	Back doors – NetBus	M
4	Back doors - Sub7	M
5	Copying of internal banking files	L
6	Destroying hardware or facilities	L
7	Planting logic bombs	M
8	Degradation / disruption of system availability	M
9	Password guessing and cracking	L
10	IP spoofing attacks	H

#	Threat	Prob
11	Man in the middle	H
12	Relay attack	H
13	TCP/IP Hijacking	H
14	DoS - Ping flood	H
15	DoS - Smurfing	H
16	DoS – Fraggle	H
17	DoS – Land	H
18	DoS – Teardrop	H
19	DoS – Bonk / Boink	H
20	DDoS	H



# Threats in *Branches* security domain

#	Threat	Prob
1	Data entry	H
2	Data editing	H
3	Installation errors	M
4	Operation errors	H
5	Deleting data	H
6	Holding data hostage	M
7	Destroying hardware or facilities	M



# Threats in *Servers / Middleware systems* security domain

#	Threat	Prob
1	Program bugs	H
2	Installation errors	M
3	Operation errors	L
4	Back doors - Back Orifice	M
5	Back doors – NetBus	M
6	Back doors - Sub7	M
7	Copying of internal banking files	M
8	Change customers' private data	M
9	Copying customer private data	M
10	Change customers' private data	M
11	Extraction of customers' private data	M
12	Holding data hostage	M
13	Changing banking data	M
14	Destroying hardware or facilities	L
15	Planting logic bombs	M
16	Degradation / disruption of system availability	M
17	Password guessing and cracking	H



# Threats in *Critical systems* security domain

#	Threat	Prob
1	Data entry	M
2	Data editing	M
3	Program bugs	M
4	Installation errors	M
5	Back doors - Back Orifice	M
6	Back doors – NetBus	M
7	Back doors - Sub7	M
8	Copying of internal banking files	M
9	Copying customer private data	M
10	Change customers' private data	M
11	Extraction of customers' private data	M
12	Changing banking data	M
13	Planting logic bombs	M
14	Degradation / disruption of system availability	L



# Threats in *Internal employees* security domain

## Employees with Desktops:

#	Threat	Prob
1	Program bugs	L
2	Installation errors	M
3	Operation errors	M
4	Deleting data	M
5	Holding data hostage	L

## Employees with Laptops:

#	13Threat	Prob
1	Program bugs	L
2	Installation errors	M
3	Operation errors	M
4	Deleting data	M
5	Holding data hostage	L
6	Spyware	H
7	Adware	H
8	Worm	H
9	Varus	H
10	Trojan horse	H
11	Remote employees' computers used as "Security bridge"	L
12	Fraud of banking information from employees' laptops	L

- **There are some banking policy - No laptop allowed to the employees;**
- **There are some banking policy - Laptops to have 2 Virtual machines – Corporate and Individual**
- **Laptops (for contractor) logically to be connected not to the banking corporate systems**



# Knowing threats, we can manage them



**Thank you !**

**Q & A**