3년의 혁신, 30년의 성장

K-ICT International Conference on Information Security (ICIS) 2015

Ceaseless Efforts to Build a Safe and Secure Cyberspace

Soojung Shin [KT CISO]

미래창조과학부 Ministry of Science, ICT and Future Planning

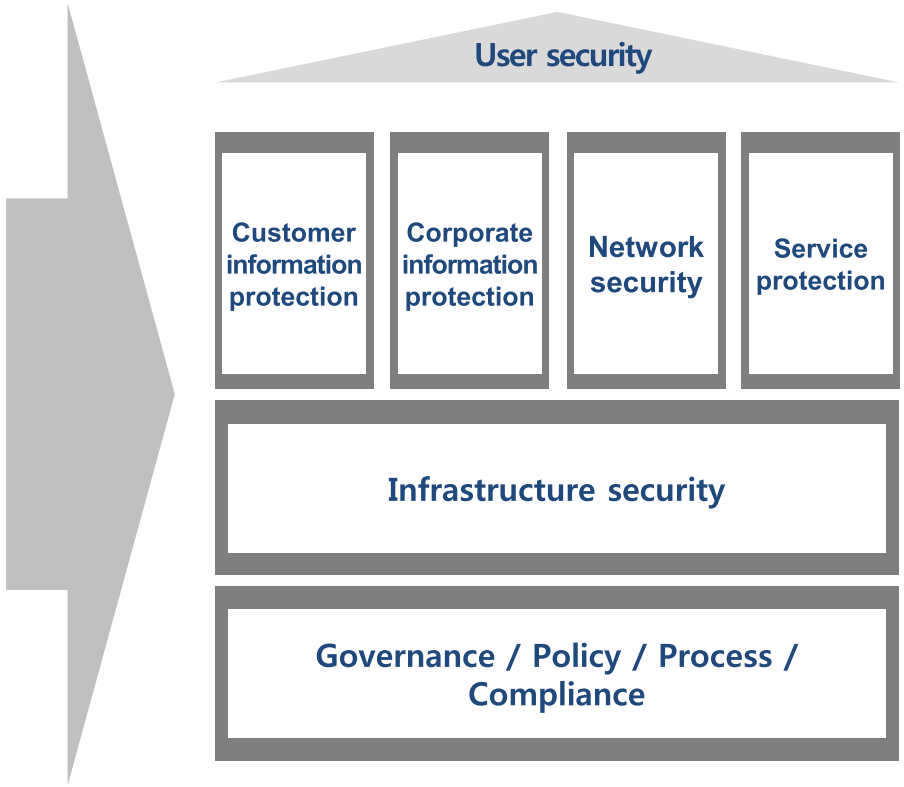
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

Contents

1. Response of Company/Organization

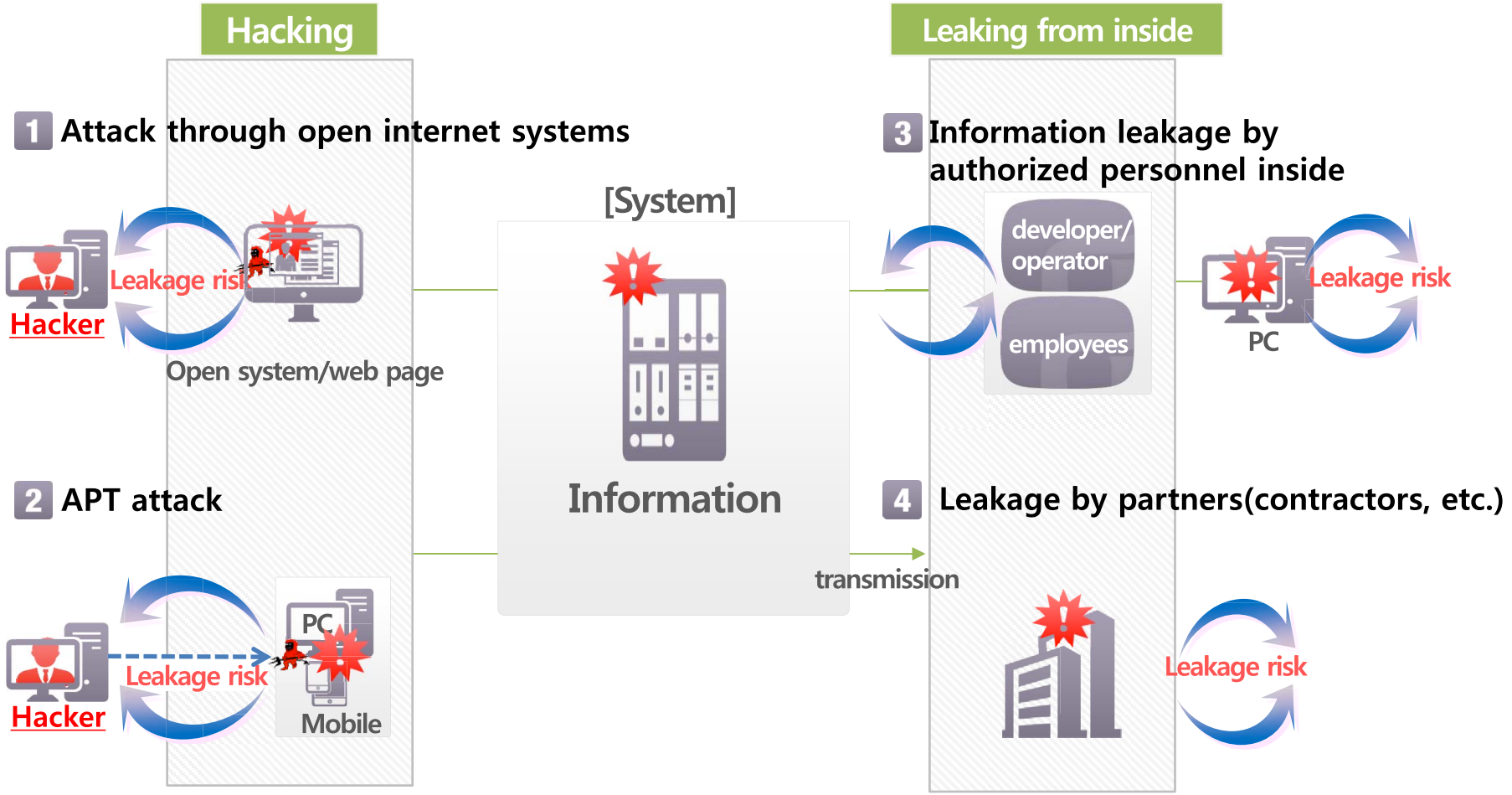
<Challenges for corporate security>

1. Changing technology
2. Changing business
3. Changing threats
4. Changing laws and regulations



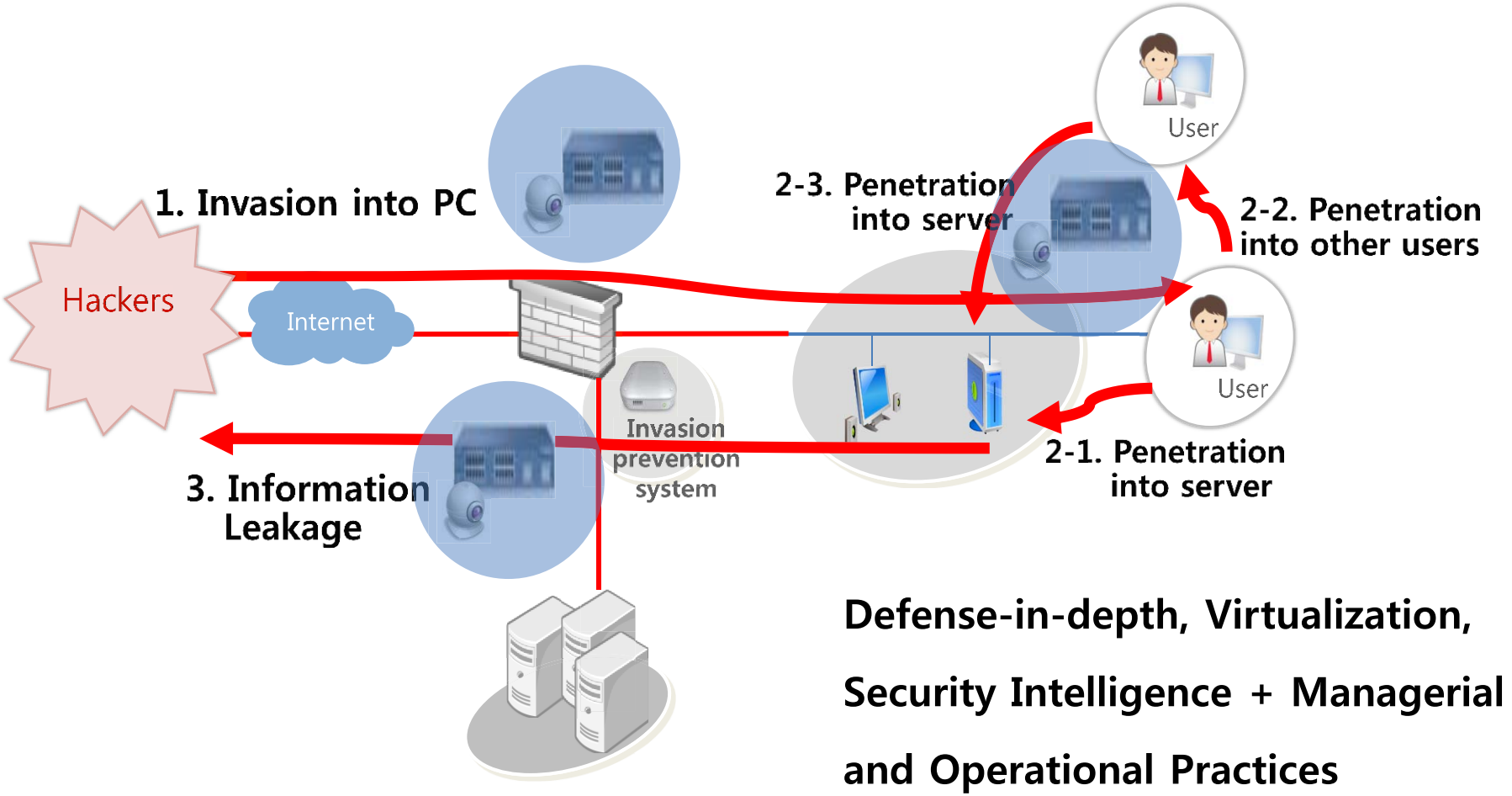
1. Response of Company/Organization

<Responding to four major risks>



1. Response of Company/Organization

<Fight against APT>

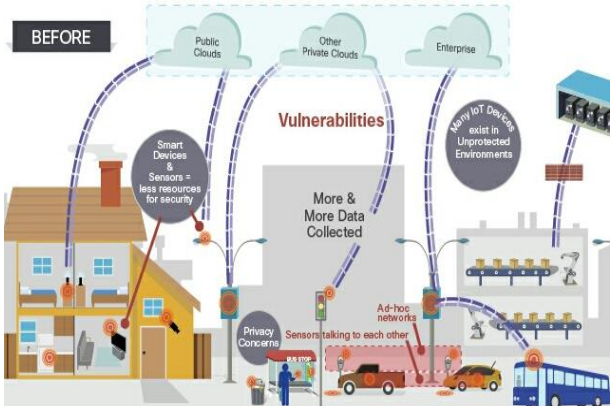


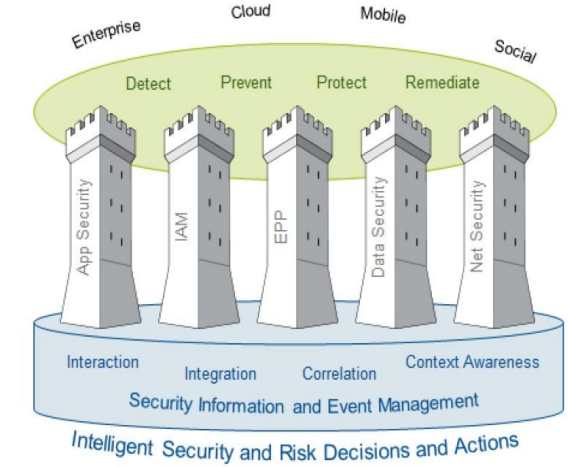
Defense-in-depth, Virtualization, Security Intelligence + Managerial and Operational Practices

1. Response of Company/Organization

<New Biz/service security>

Web, IoT, Big data, Social, Fin-Tech, 5G…





EPP = endpoint protection platform; IAM = identity and access management

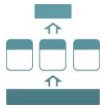
Source: Gartner, Inc.

Embedded Security

Use vs. Protection
Speed vs. Assurance

1. Response of Company/Organization

<Changing Action Strategy – 3 responding strategies & 2 bases>

	① Defense → Minimize spreading and damage even after being penetrated → Resilience
	② Various security solutions → Security Analysis/Intelligence
	③ IT-oriented security → security embedded in Biz, security for all members
	Narrow down the perimeters
	Visualize assets and risks

2. Response of Society

Will society be safe if each organization establishes the best security measures?

Gridlock

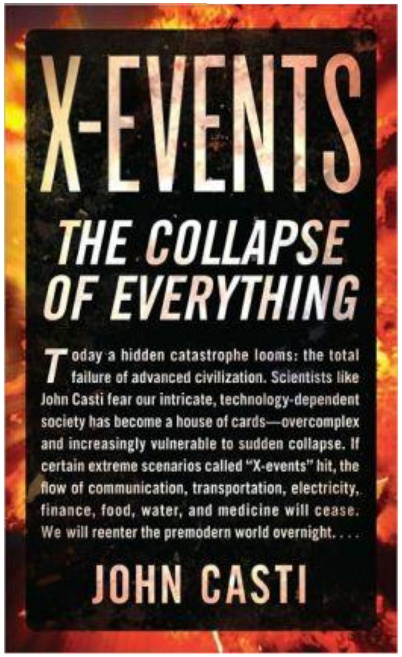
- **Small companies that do not feel the need to invest in security**
- **Small companies/organizations with great security risks**
- **Security cultual of social members**
- **Information sharing**
- **Matters with other countries**

2. Response of Society

<National-level big security risks and X events of security area>

1. Internet paralyzed by DDoS attack
2. Penetration into infrastructure
3. Client paralyzed by extensive Botnet attacks
4. Large-scale credit card fraud

Source: Edward Skoudis



No 1. Widespread outage of Internet among 11 X events
(c.f. No 8. Communicable disease)
-Limit of the Internet structure
-Intentional attack

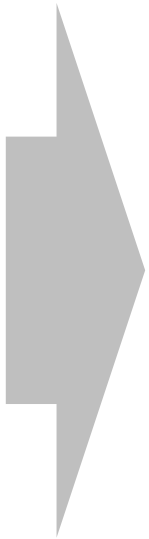
Responding scenario and readiness

2. Response of Society

<Promoting people's awareness>

People insensitive to risks and principles

Insufficient security measures taken by people



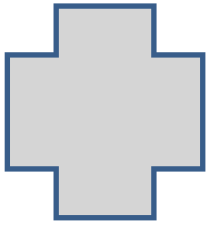
Promoting awareness as strongly and extensively as, for example, the no-smoking , no-drunk driving campaign

3. Other Issues

Motive of most attacks: Money

→ Most companies have measures against this risk.

→ Cost-effective response is possible to a degree.



Other motives?

- Social disorder
- Internet attack
- Wiretapping
- National perspective

→ Most companies have difficulties in cost-effective responses.

→ Cyberspace is mixed, unlike the physical world.

→ Difficult to defend

- National security defense strategy aligned with civil security strategy
- Cooperation between national defense and security companies
- Offensive competitiveness

4. Big Questions that Industries & Academia Need to Answer

- How exactly to detect real attacks/infringement minimizing false-positives and respond to them as soon as possible ?
- How to predict the attacks?
- Confrontational techniques active to the changes in threats and vulnerabilities?
- Innovative authentication & trust model?
- Innovative privacy protection techniques?
- Innovative approach for guaranteeing secure and resilient networks? …

<Constraints>

- Security that is less bothersome for users' task performance
- Security that is not too complicated for its management

5. Conclusions

- Simplification
- Visualization
- Adaptability
- Resilience
- Slack/Backup/Over investment