# Renovating our security management:
## New ways to protect your infrastructure

Suguru Yamaguchi
Nara Institute of Science and Technology
Japan

# Overview

- Discuss 2 topics about Security Management

1. How can we make more manageable infrastructure in terms of security? Or, how can we reduce the security incidents?

2. How can we work effectively at incident response?

# #1: reducing security incidents

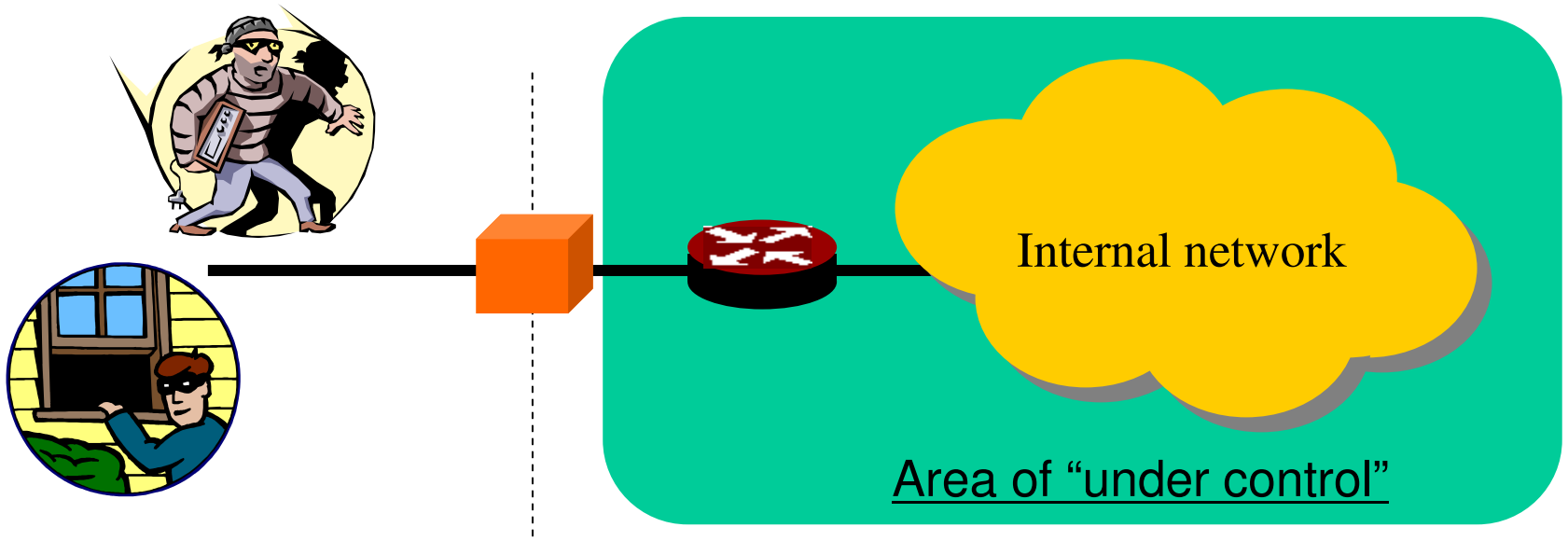
# Observations

- Few organizations that do nothing for security management on their Internet / Intranet infrastructure.
  - Many organizations have their own security policy.
  - Installation and operation of “Firewall” is quite common.
  - Introducing anti-Virus / anti-Worm software is the way of “minimum protection” of your working environment
  - Awareness program to let people know there are so many criminals, barbarians and bad guys in the Internet

- Still many security incidents can be observed and the number of incidents is getting increased.

# Our security management model, So far

- Perimeter Defense / Boarder Protection




FEBA: Fighting Edge of Battle Area, perimeter / boarder

# Assumptions in this model

- Clear but implicit separation of Inside (Intranet) and Outside (Internet)
  - Every “bad thing” comes from the outside.
  - The inside is 100% safe place.
  - No one inside does not have any hostile actions against the management.
  - Therefore, it is quite good idea to define the perimeter / boarder and to concentrate counter measures on the boarder.
    - Cost effective way of defense
    - Strong enough to protect the Inside

# The model is good enough for today? (1)

- Many security troubles in the Inside
  - Epidemic of Virus / Worm infections
  - Broad distribution of malicious code via E-mails
  - Bringing back viruses via Laptop PC
  - Executing malicious code via WWW accesses
  - Malicious code injection by P2P tools

- Troubles caused by our people
  - Regardless of intentional / non-intentional
  - Various types of “users”
  - Various types of “use”
  - How can we make the inside “under control”? Or, do you have any ways to know what your people is doing?

# The mode is good enough for today? (2)

- Firewall on the perimeter is not working effectively.
  - Not fit well to new services
    - especially P2P applications (e.g. VoIP)
  - Packet forwarding performance degradation at the firewall
    - Does not get “wire speed” via firewall
    - Applications need high performance are now proliferating
    - Ex. How can we make the firewall for 10GbE
  - The best way to protect your infrastructure is to stop your packet forwarding and relay via proxies.
    - Aggressive use of application level gateway.
    - RIDICULOUS!

# We need new solutions!

- We need new security management model
  - Requirement
  1. The model assumes that vulnerabilities are existing even inside the target infrastructure.
  2. The model have to have a mechanism to regulate the expansion of security incidents, especially against infectious incidents like Worms.
  3. Users can enjoy the leading edge “cool” applications even with the security management.
  4. Performance cannot be sacrificed with the reasons of “security management”.

# Don’t forget it! (1)

- Systems for each individuals have to be managed more than now.
  - Vulnerability is always sitting on users’ systems
  - Users’ systems are not on the boarder but in inside.
  - Need to manage more users’ system.
  - Revisit to the question again:
    - Do we have to give full functional, general purpose computing platform with general purpose applications for everyone in your organization?
    - How can we manage 100% all the computing platform in our organization?
    - Can we accept the use of Laptop PC’s?

- Ideas
  - Less variety of platforms
  - Provide application (e.g. WWW) platform for “routine” works
  - More management on the mobility of users, e.g. laptop PC management

# Don't forget it! (2)

- Capability management is the base
  - Who can do what?
  - What kind of information you can look into?

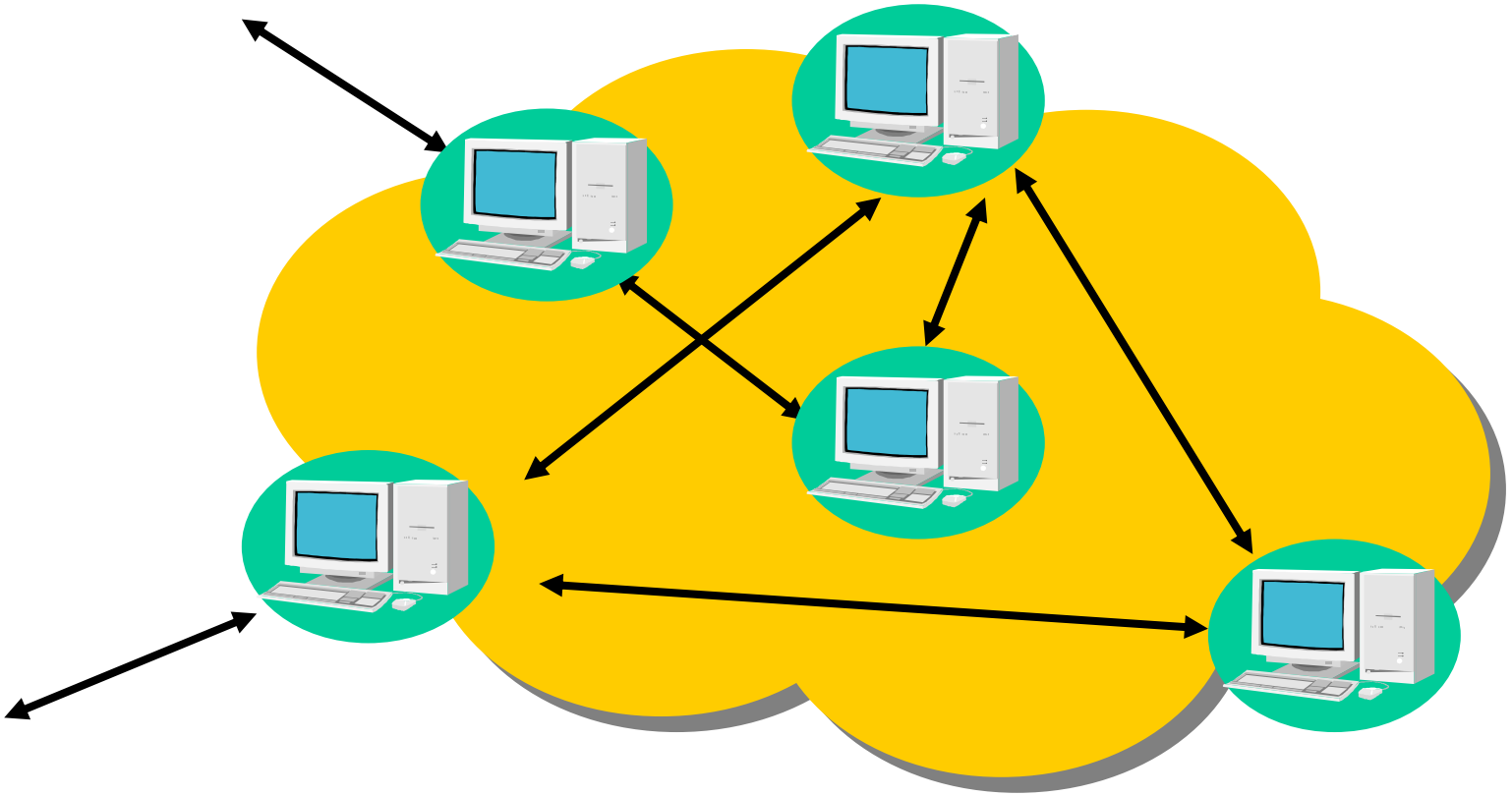
$$f(perm(user), class(document)) = \begin{cases} 00 & deny \\ 01 & read \\ 10 & write \\ 11 & read \,\&\, write \end{cases}$$

  - Consistent and maintain their integrity
  - Fit to actual work environment
  - Use technologies:
    - LDAP? RBAC? AAA? ….

# Two options…

- Maximizing the protection on each system.
  - Set a boarder around each system.
  - No boarder / perimeter strategy
- Maximizing the management of traffic / use of applications and separating malicious activities.
  - Sophisticated control of “boarder”
  - Once on the edge of the Intranet, but at the other time, the boarder is around your system.

# Maximizing the protection on each system

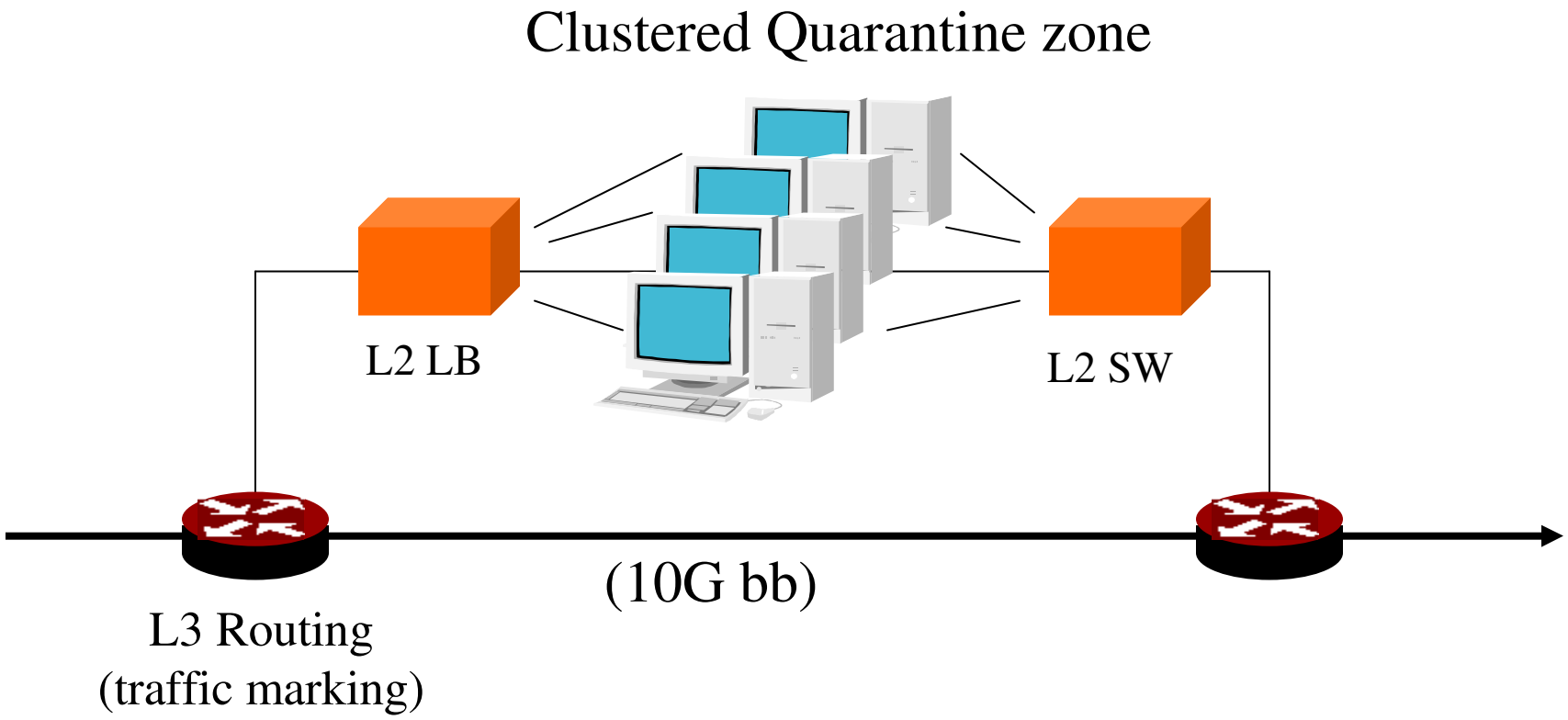


# Managed communications

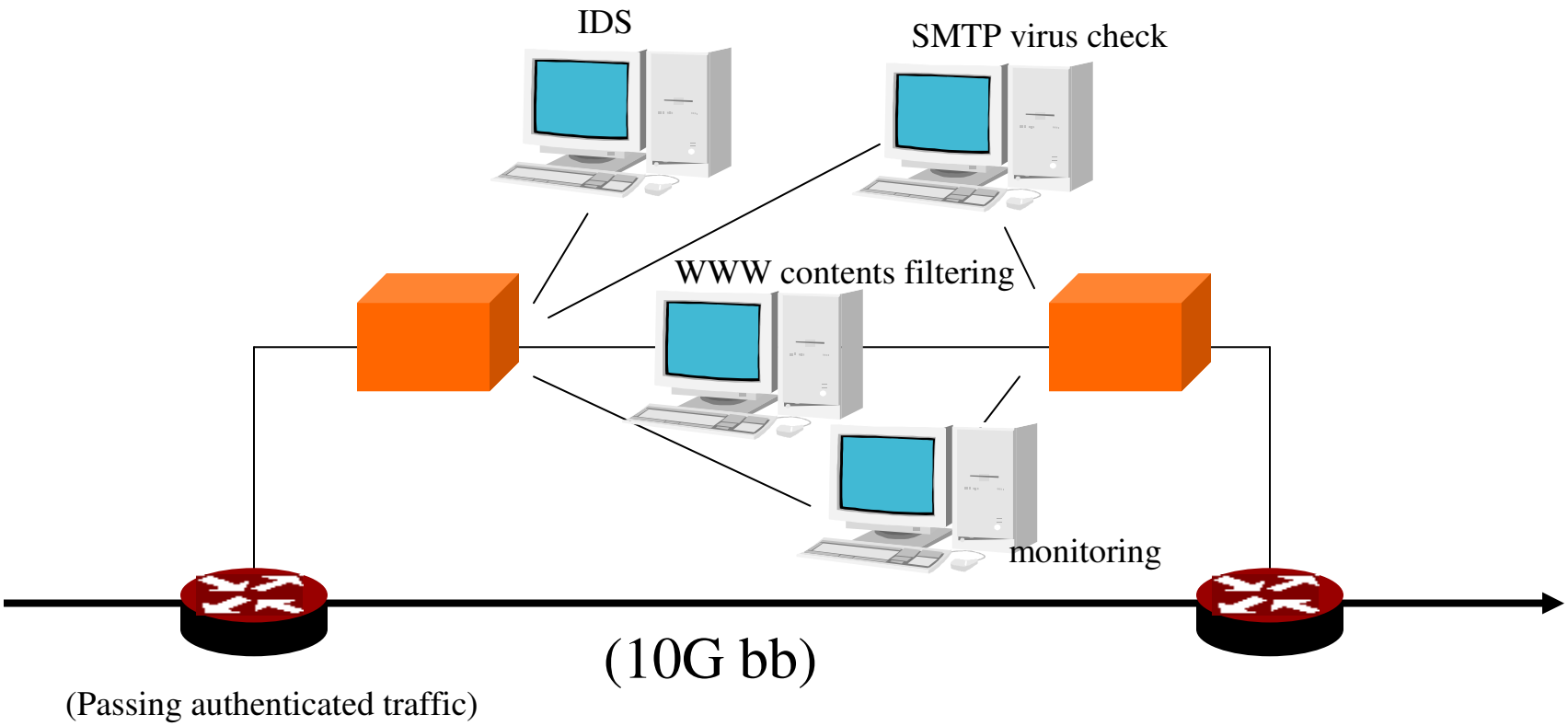
- Each system is protected as much as possible.
- Employing “security policy”
  - Definition of the role of each system
  - Definition of AUP
  - Definition of acceptable communication, access, and use
  - Managing every communication, access and use precisely.
- Possible!
  - It is quite rare for everyone to contact any machines in your environment.
    - Normally, web proxy, mail server, ….
    - Limited number of candidate, ….
  - More manageability on communication devices
    - Access switch, routers, …

# High performance firewalls

- Clustered firewall
  - Quarantine

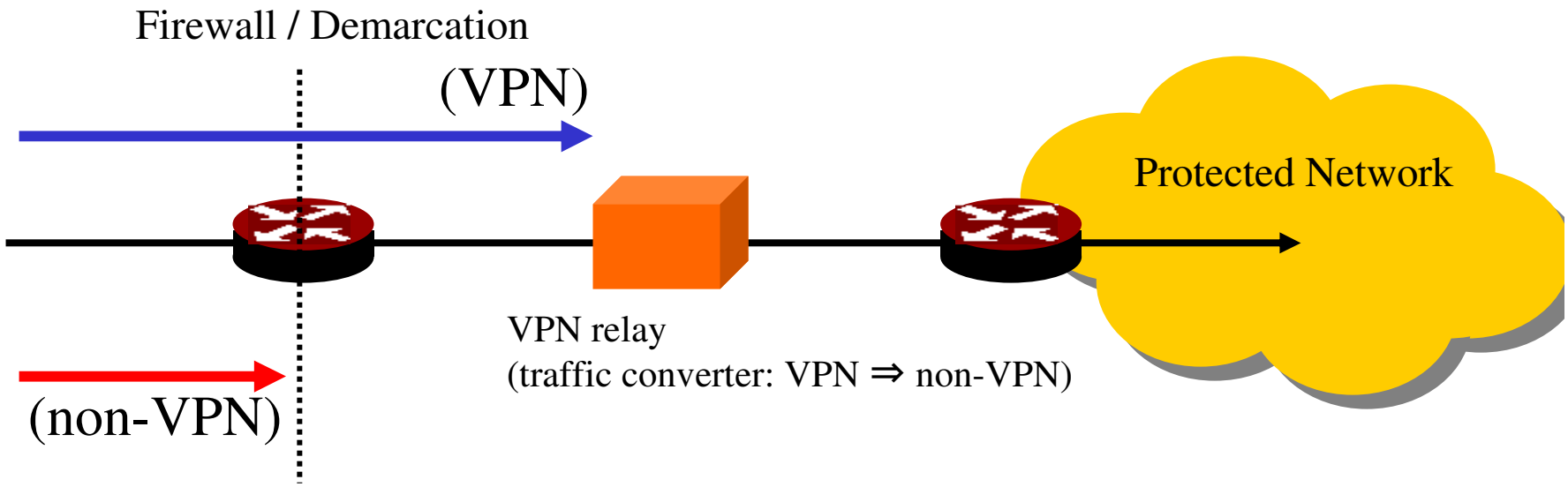


# Functional distribution on the quarantine



# Technique for keeping it works fine!

- Traffic marking
  - Less overhead of filtering and diverting the traffic
    - Pattern matching is not so good on L3 switch
  - Marking the traffic
    - Simple ways to mark “candidate” to be passed through FW
    - Less overhead for marking
  - Current candidate: VPN



# However, ....

- Still no clear shape on the “new” security management model
  - We need more “best practice”
  - We need more expertise.
  - Need more time to make feedback from the operation.
  - Our first step for the second generation of Security Management.

# #2: high performance incident response

# Observations

- Security management in many organization seems to be okay.

- However, once a security incident arise, always quite long period is needed to settle the trouble.
  - Low response ability.
  - Not only by technology / engineering, but also by organization itself.
  - What's high performance incident response and how can we make it?

# Security Management

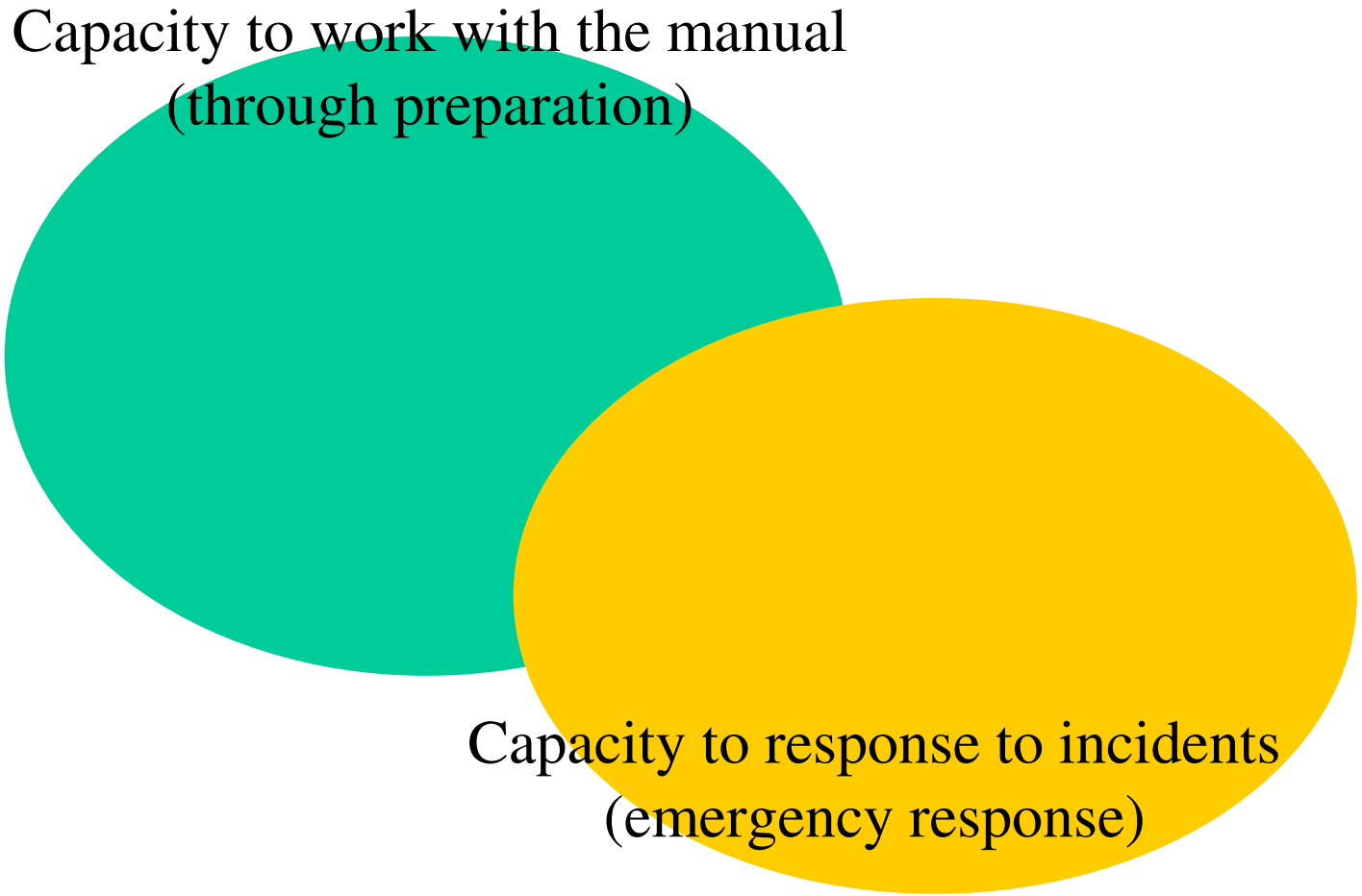
- Make preparation for the risk we know.
  - Develop the routine to act against risks
  - We know the risk through “risk assessment” process.
- We cannot prepare for everything
  - Cost
  - Technology
  - Imagination

# Pit hole in security management

- "Well prepared"
  - Act very well against risks we know
  - Forget the fact that there are other risks we don't know
  - Masking effect

- We try to prepare more…
  - Masking effect working very well
  - Try to prepare more sophisticated way.
    - Adding 100 pages to security management manuals !?
  - Not work well once encounter to unknown trouble arise.

# Two capability needed



# Help for emergency response

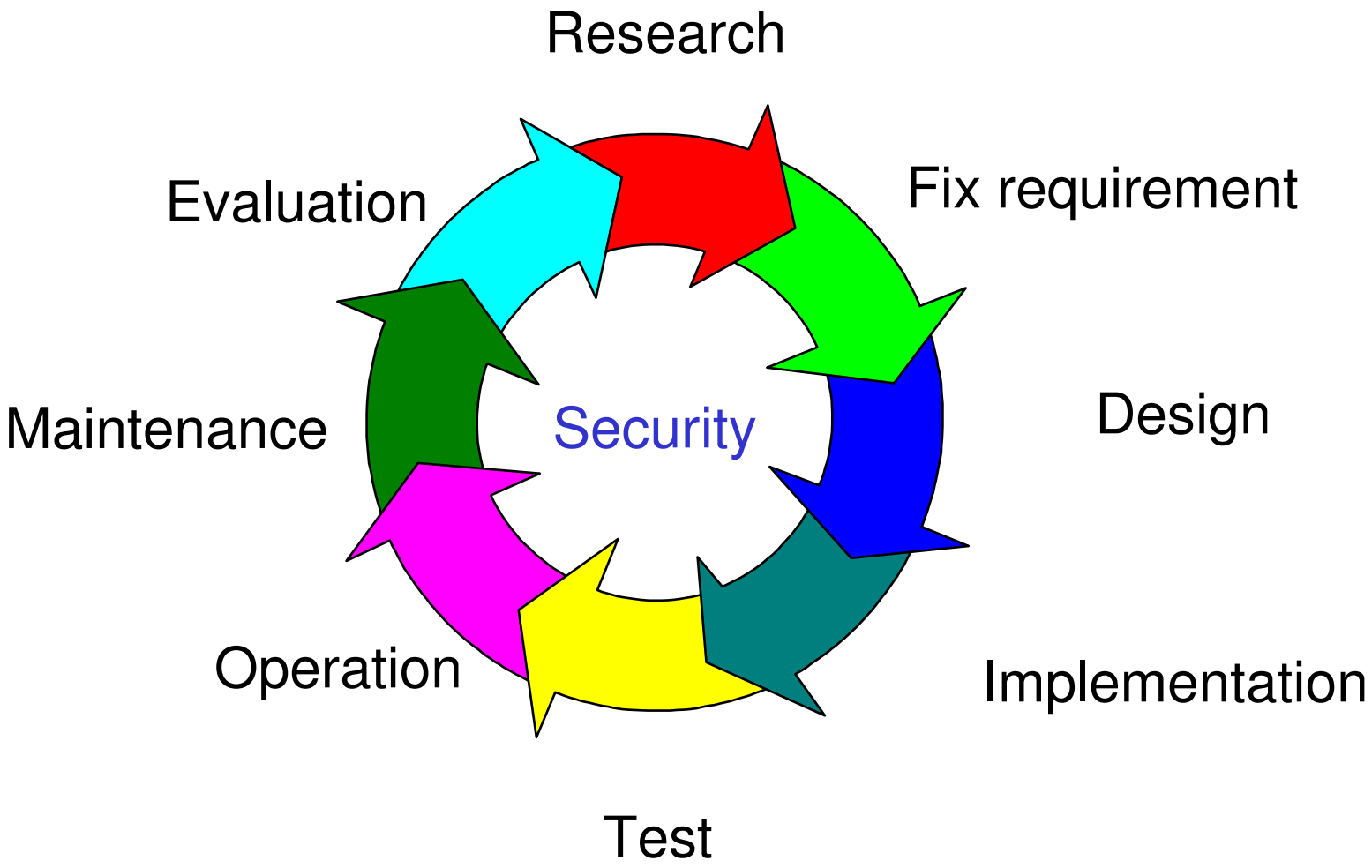
- Estimate the loss or effect by the troubles
- Stop expanding the trouble
- Generate multiple ad-hoc counter measures in time
- Remember the trouble and its reason, and keep it in memory.
- Study more on troubles
- More professionals on the matter

# What we have to explore

- The way to improve these two capabilities
- The way to co-exist these two capability

- High Reliability Organizations: HRO

# The model, fit only to “preparation”



# We need another model.

- Model for improving the capability of “response”
  - Wider view on the problem
  - Professional expertise and capability on the problem
  - Clear delegation of responsibility
  - Information management and sharing

- But still we don’t know….

# Summary

- Discuss 2 topics related to security management
  - new step for 2nd generation of Security Management
  - Preparation and response

- We don't have clear answer at this moment
  - We need to share more expertise
  - Best practice
  - At various opportunity: IETF, International conferences, operators' conferences, ….