


Security Incidents


- Security is problem that cannot be solved completely by network defenses.
- These Problems include
 - System Failure (unscheduled downtime)
 - Insider Threat
 - Software Flaws



3

The Responsibilities of CERT Organizations

- Incident Handling
 - to provide a centralized contact on computer and network security incident reporting and response for local enterprises and Internet users in case of security incidents
 - Reactive
- Can We Prevent Incidents From Occurring?



4

Incident & Vulnerability

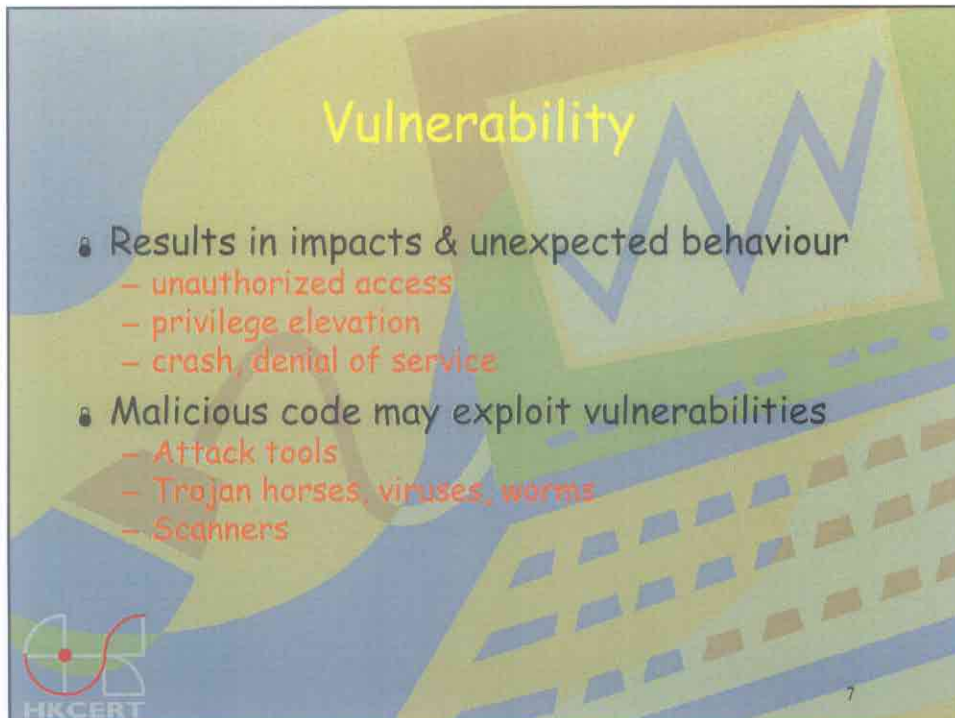
- HKCERT received more than 4,000 incident reports in 2004
- More than half are related to vulnerability
 - Sasser Worm
 - Un-patched systems

5

Vulnerability

- The result of a combination of Issues
 - Software Defects
 - Implementation Flaws
 - Design Inadequacies
 - Environmental Adaptation
 - Complex Interactions
- Leads to failure of confidentiality, integrity or availability; violation of security policy

6



Vulnerability

- Results in impacts & unexpected behaviour
 - unauthorized access
 - privilege elevation
 - crash, denial of service
- Malicious code may exploit vulnerabilities
 - Attack tools
 - Trojan horses, viruses, worms
 - Scanners

HKCERT 7



Impact of Vulnerability

- Critical infrastructure affected
 - Government
 - Financial
- Direct costs
 - downtime, lost revenue, outright theft
 - transportation, communication, supply system disruption
 - recovery costs
- Indirect costs
 - consumer confidence (phishing, on-line banking, e-commerce)

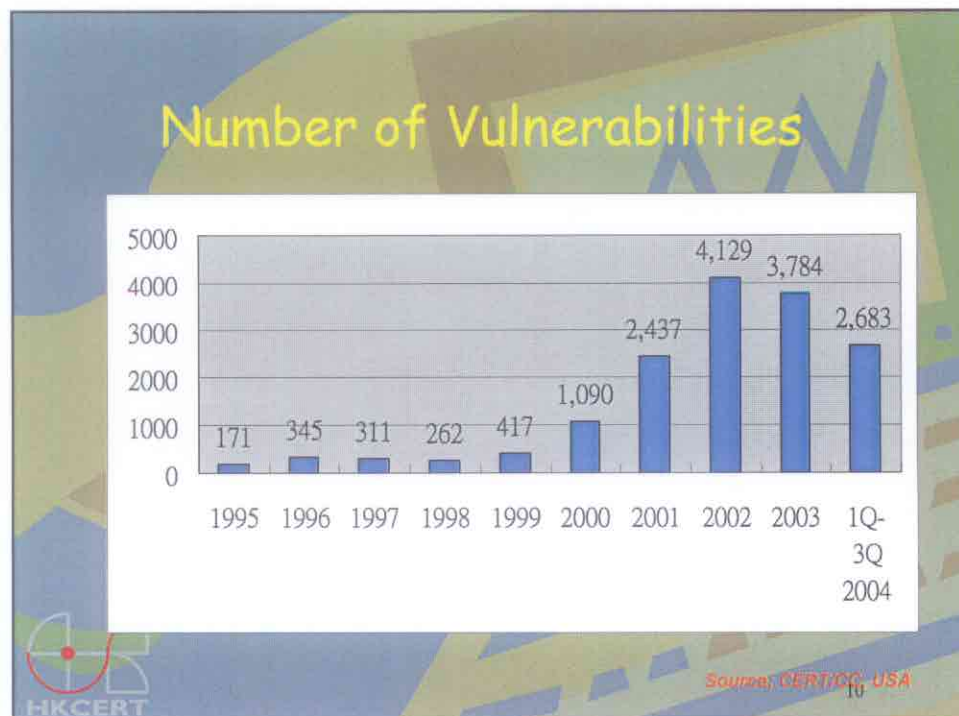
HKCERT 8

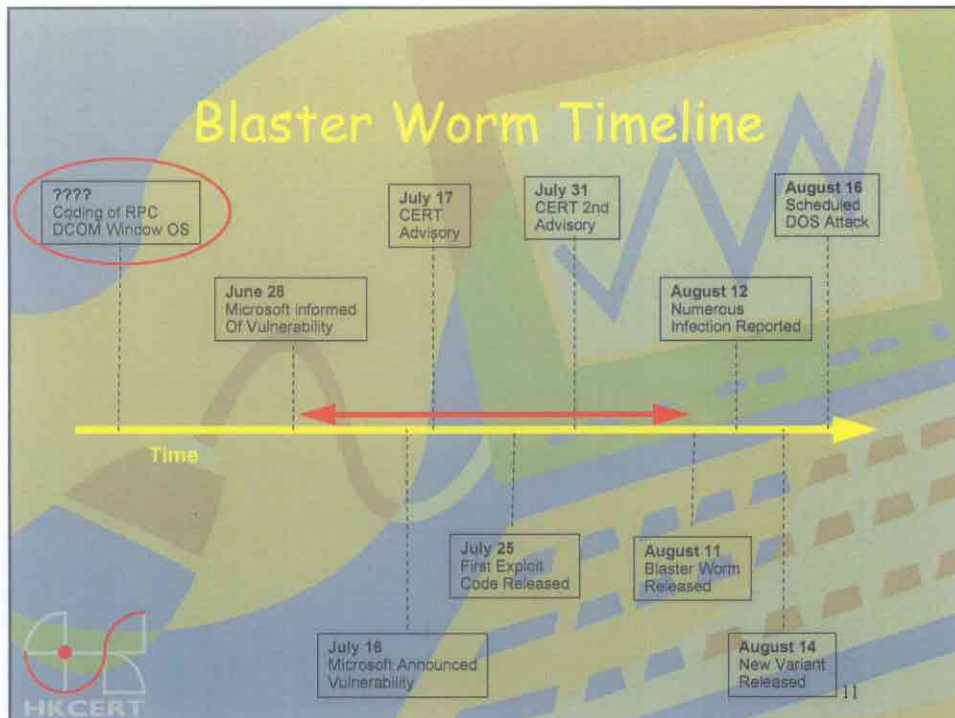
Cost of Ownership

- Purchase Price
- Cost of Security Breaches
 - Damages
 - Recovery Costs
- Cost of Security Prevention
 - Patch Management



9



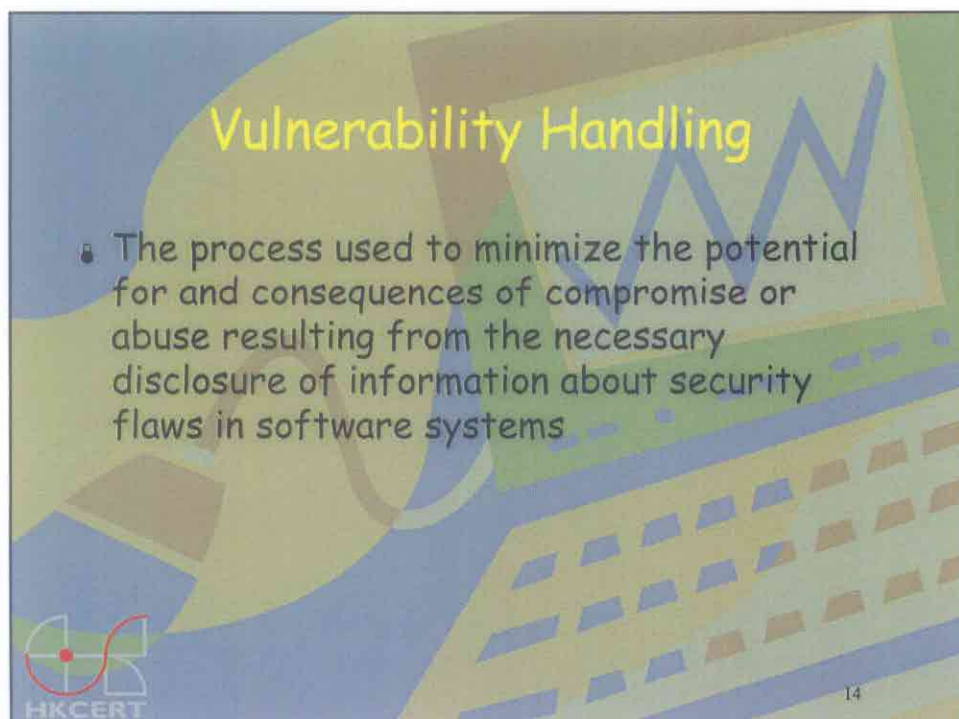
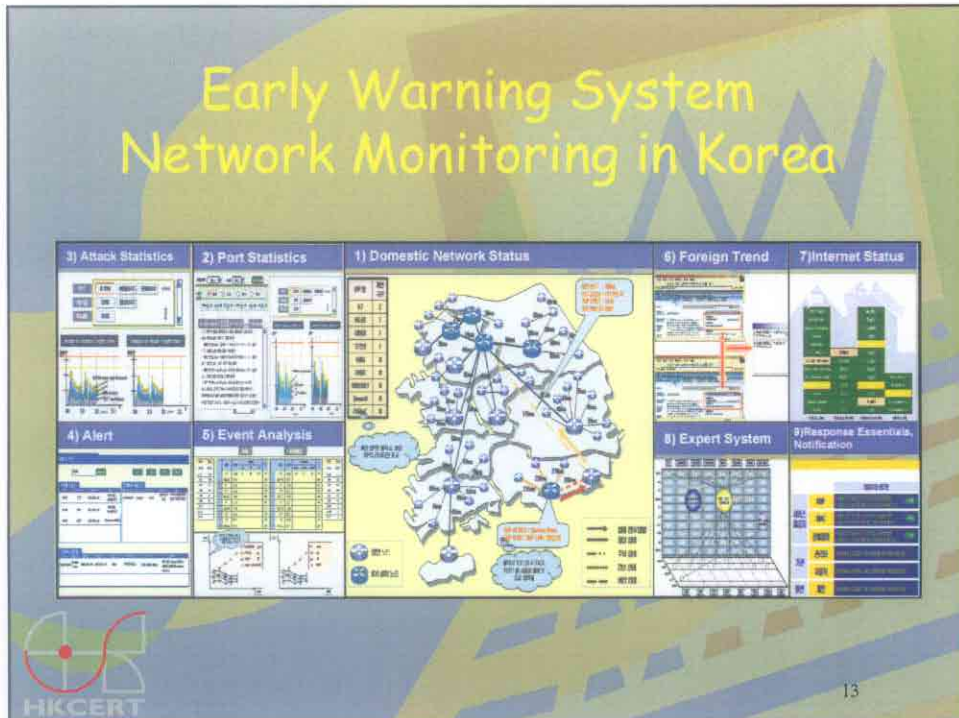


Can We Prevent Incidents From Occurring?

- Early Warning Systems
 - Network Traffic Monitoring (Volume)
 - Abnormal Packets (Contents)
- Vulnerability Handling
- Vulnerability Analysis & Prevention

HKCERT

12

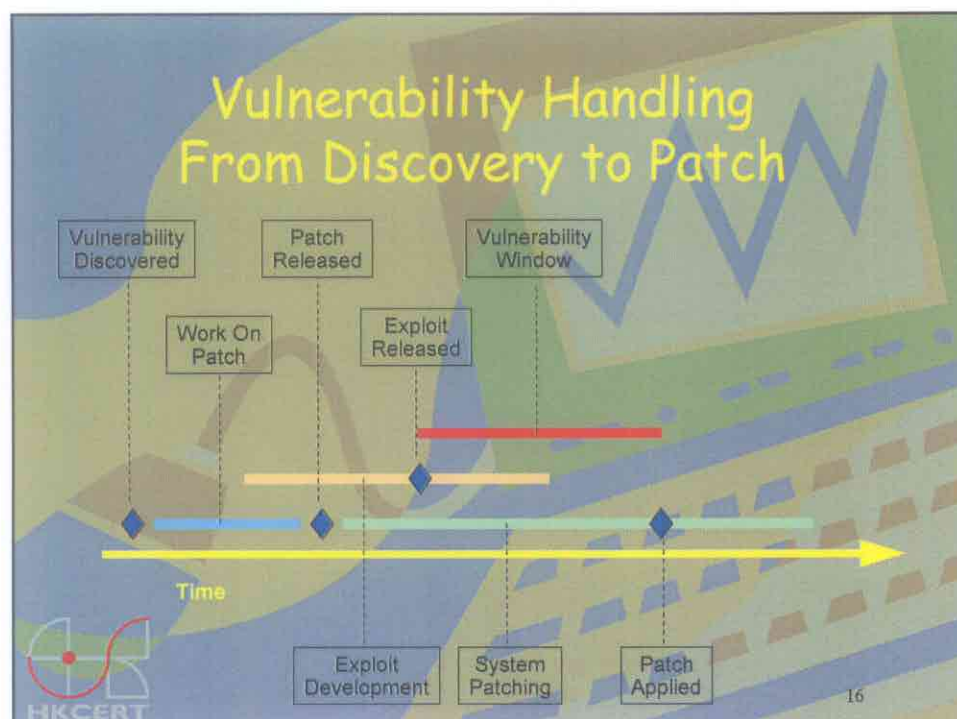


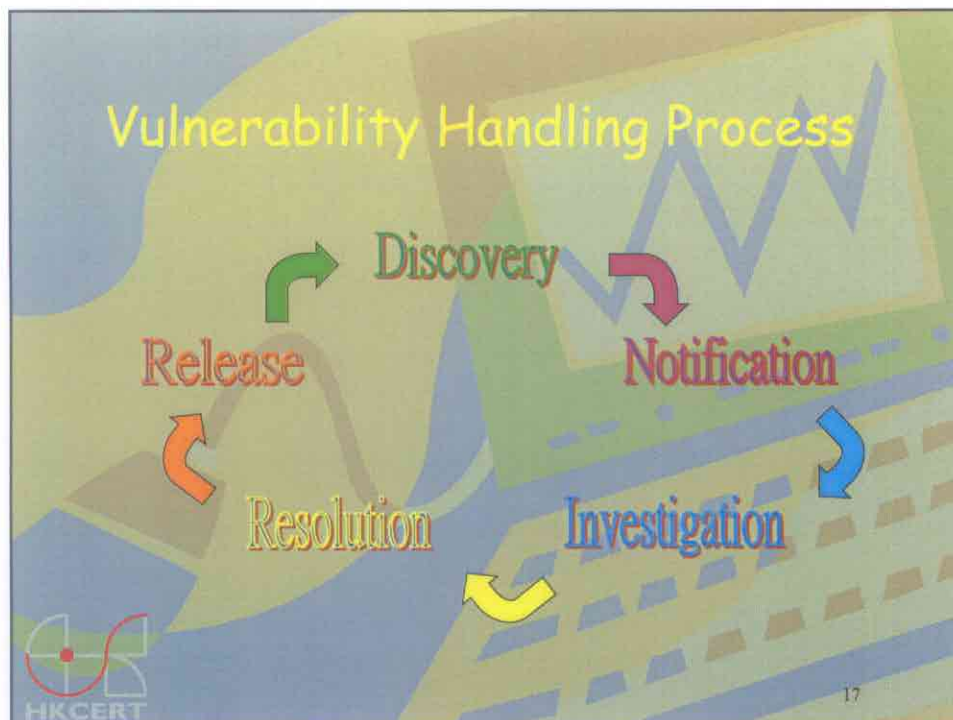
Vulnerability Handling

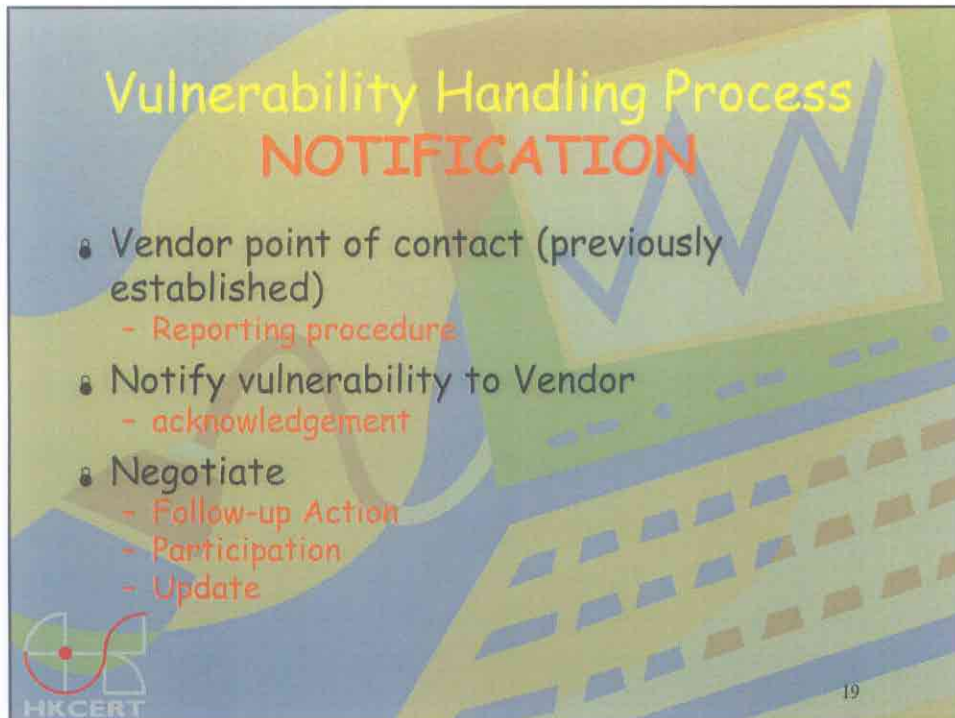
- Minimize Consequences
 - Advise in Advance
- Disclosure
 - All Vulnerability of General Purpose Software must be disclosed
 - Encourage to apply patches
- The Public need to understand
 - Consequences
 - Preconditions
 - Remediation



15







Vulnerability Handling Process
NOTIFICATION

- Vendor point of contact (previously established)
 - Reporting procedure
- Notify vulnerability to Vendor
 - acknowledgement
- Negotiate
 - Follow-up Action
 - Participation
 - Update

HKCERT 19



Vulnerability Handling Process
INVESTIGATION

- Vendor investigate vulnerability
- Parties collaborate
 - Regular updates
 - Additional Information Exchange
- Vendor share detailed results
 - Confirmed: Build remedy
 - Disproved: Supporting information
 - Unable to confirm/disprove: Further research, exchange of information

HKCERT 20



Vulnerability Handling Process
RESOLUTION

- Confirmed Vulnerability -
 - Take remedy action
 - Maintenance release
 - Configuration Change - patch
 - Temporary workaround
- Patch & Advisory Release
 - Early Release
 - Draft advisory

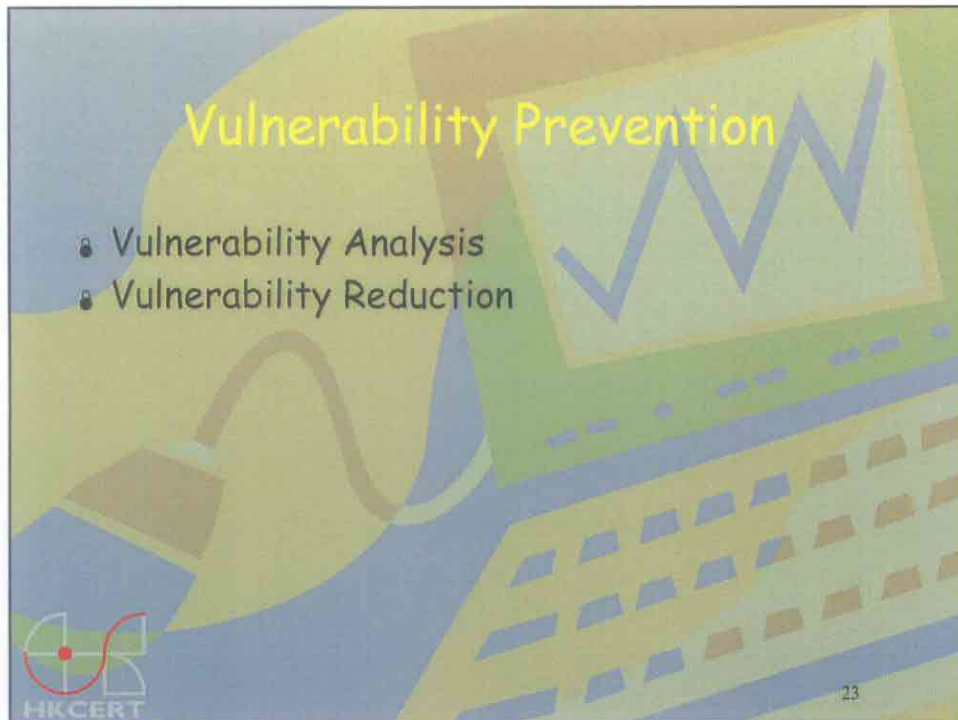
HKCERT 21



Vulnerability Handling Process
RELEASE

- Remediation
 - documentation
 - Patches release
- Full disclosure
 - Affected products
 - Risks associated
 - User Actions
 - Known side effect

HKCERT 22

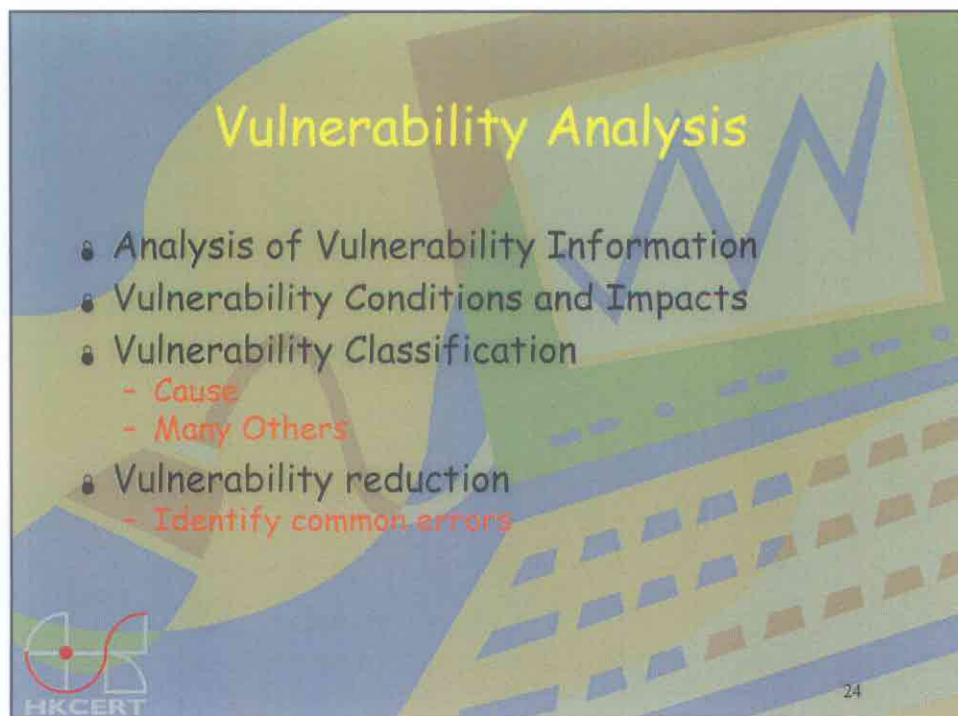


Vulnerability Prevention

- Vulnerability Analysis
- Vulnerability Reduction

HKCERT 23

The slide features a background illustration of a computer monitor displaying a line graph with a blue zigzag line, and a keyboard below it. The HKCERT logo is in the bottom left corner.

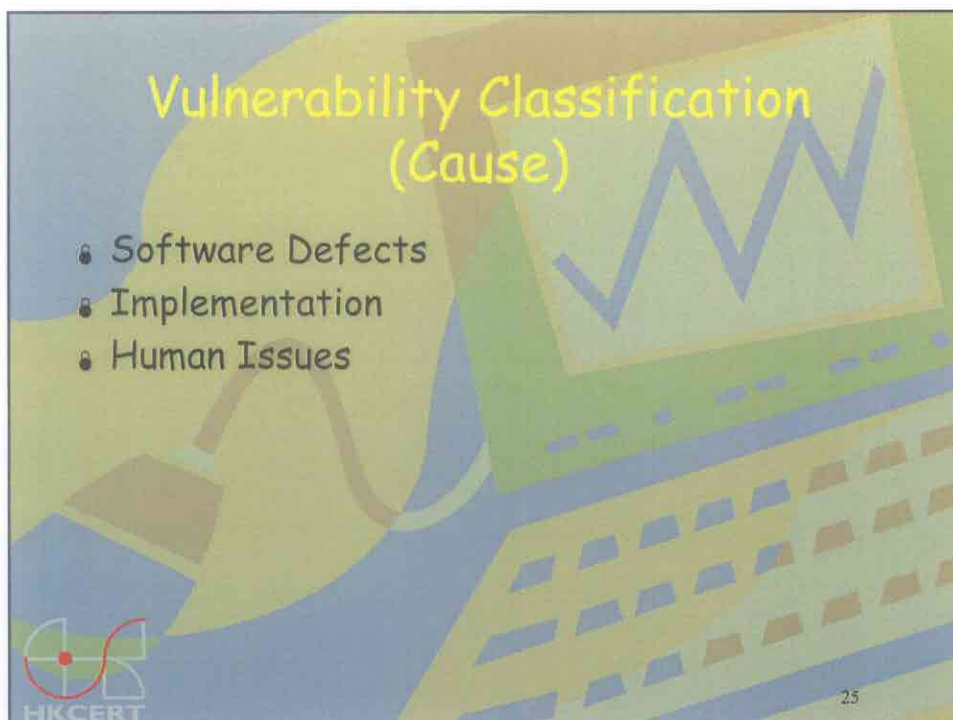


Vulnerability Analysis

- Analysis of Vulnerability Information
- Vulnerability Conditions and Impacts
- Vulnerability Classification
 - Cause
 - Many Others
- Vulnerability reduction
 - Identify common errors

HKCERT 24

The slide features a background illustration of a computer monitor displaying a line graph with a blue zigzag line, and a keyboard below it. The HKCERT logo is in the bottom left corner.

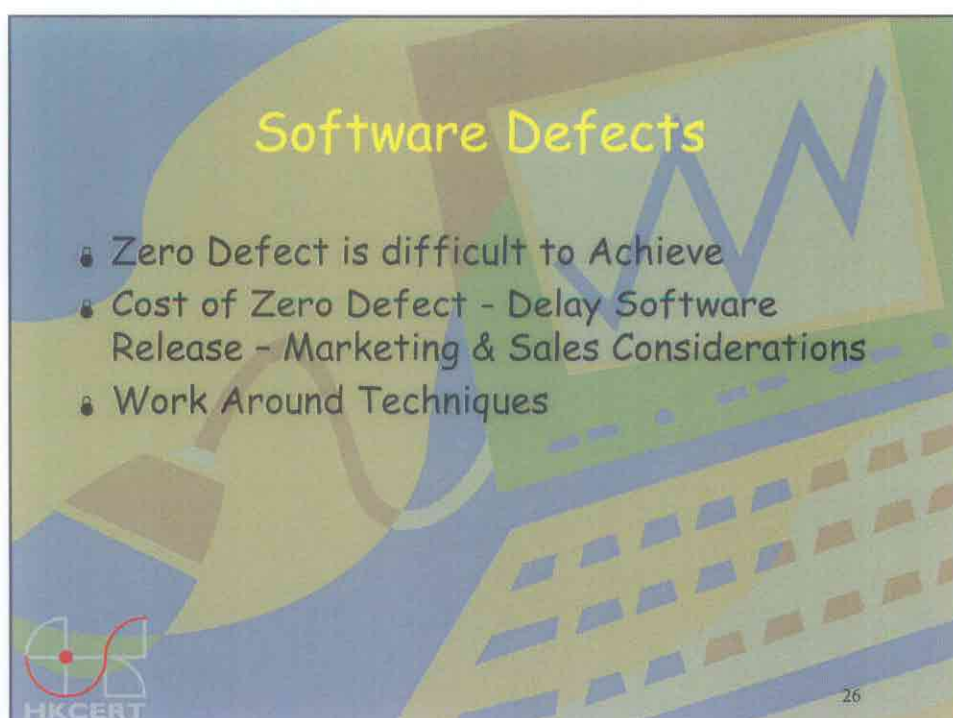


**Vulnerability Classification
(Cause)**

- Software Defects
- Implementation
- Human Issues

HKCERT 25

The slide features a background with abstract shapes in shades of blue, green, and yellow. A line graph with a blue line is visible in the upper right quadrant. The HKCERT logo is in the bottom left corner, and the number 25 is in the bottom right corner.



Software Defects

- Zero Defect is difficult to Achieve
- Cost of Zero Defect - Delay Software Release - Marketing & Sales Considerations
- Work Around Techniques

HKCERT 26


The slide features a background with abstract shapes in shades of blue, green, and yellow. A line graph with a blue line is visible in the upper right quadrant. The HKCERT logo is in the bottom left corner, and the number 26 is in the bottom right corner.

The slide features a background with a stylized laptop and keyboard. A line graph on the laptop screen shows a fluctuating blue line. The title 'Software Defects' is in yellow. The content is a bulleted list with sub-points in red. The HKCERT logo is in the bottom left, and the number 27 is in the bottom right.

Software Defects

- Software Complexity
 - Difficult to design
 - Difficult to manage software development
 - Error-prone
- Compatibility
- Software Changes
 - New Features
 - Bug Fix
- Performance
- Best Practices

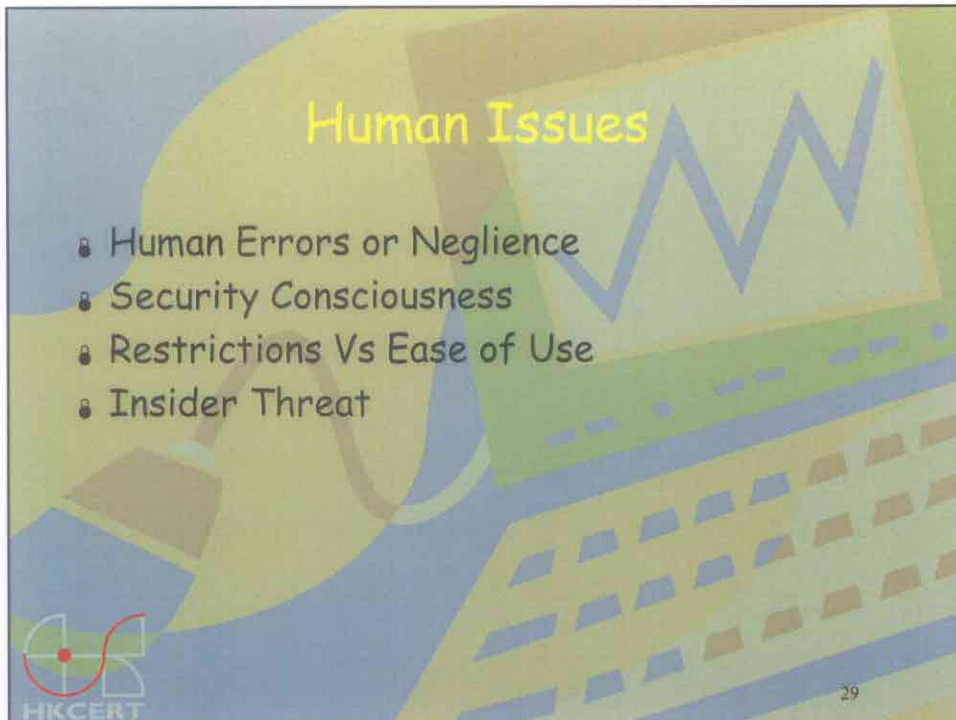
HKCERT 27

The slide features a background with a stylized laptop and keyboard. A line graph on the laptop screen shows a fluctuating blue line. The title 'Implementation' is in yellow. The content is a bulleted list with sub-points in red. The HKCERT logo is in the bottom left, and the number 28 is in the bottom right.

Implementation

- Installation & Configuration
- Proper Management
 - Regular Updates

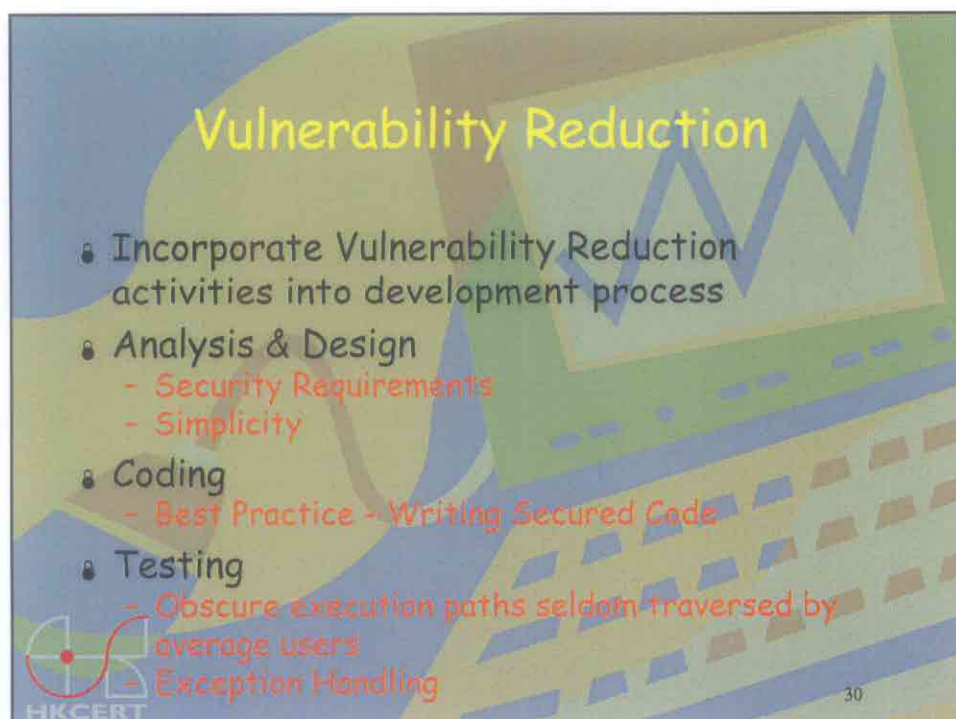
HKCERT 28



The slide features a background with abstract shapes in shades of blue, green, and yellow. A line graph with a blue line is visible in the upper right. The HKCERT logo is in the bottom left, and the number 29 is in the bottom right.

Human Issues

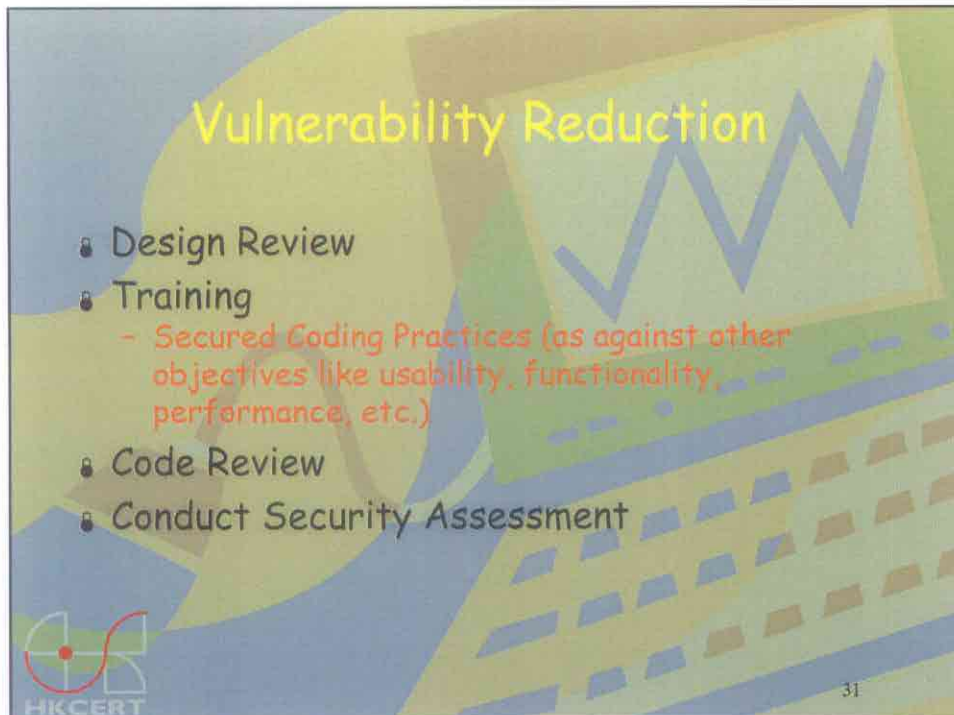
- Human Errors or Negligence
- Security Consciousness
- Restrictions Vs Ease of Use
- Insider Threat



The slide features a background with abstract shapes in shades of blue, green, and yellow. A line graph with a blue line is visible in the upper right. The HKCERT logo is in the bottom left, and the number 30 is in the bottom right.

Vulnerability Reduction

- Incorporate Vulnerability Reduction activities into development process
- Analysis & Design
 - Security Requirements
 - Simplicity
- Coding
 - Best Practice - Writing Secured Code
- Testing
 - Obscure execution paths seldom traversed by average users
 - Exception Handling



Vulnerability Reduction

- Design Review
- Training
 - Secured Coding Practices (as against other objectives like usability, functionality, performance, etc.)
- Code Review
- Conduct Security Assessment

HKCERT 31

The slide features a background with a blue line graph showing an upward trend, overlaid on a keyboard. The HKCERT logo is in the bottom left corner.



Implications to Vendors

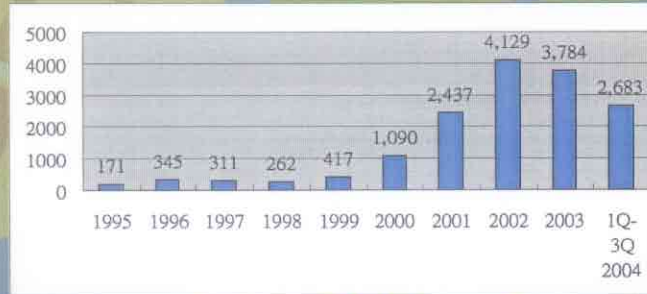
- More Effort (and thus Cost) on
 - Training
 - Third Party Assessment
 - More Testing
- Technical Difficulties
 - Testing for software security is more time consuming than functional testing
- What is the measurement for Security?
 - How do we know that the security features are adequately tested

HKCERT 32

The slide features a background with a blue line graph showing an upward trend, overlaid on a keyboard. The HKCERT logo is in the bottom left corner.

Implications to Vendors

- Reduce Support Effort
- Image Building
- Reduce Vulnerabilities



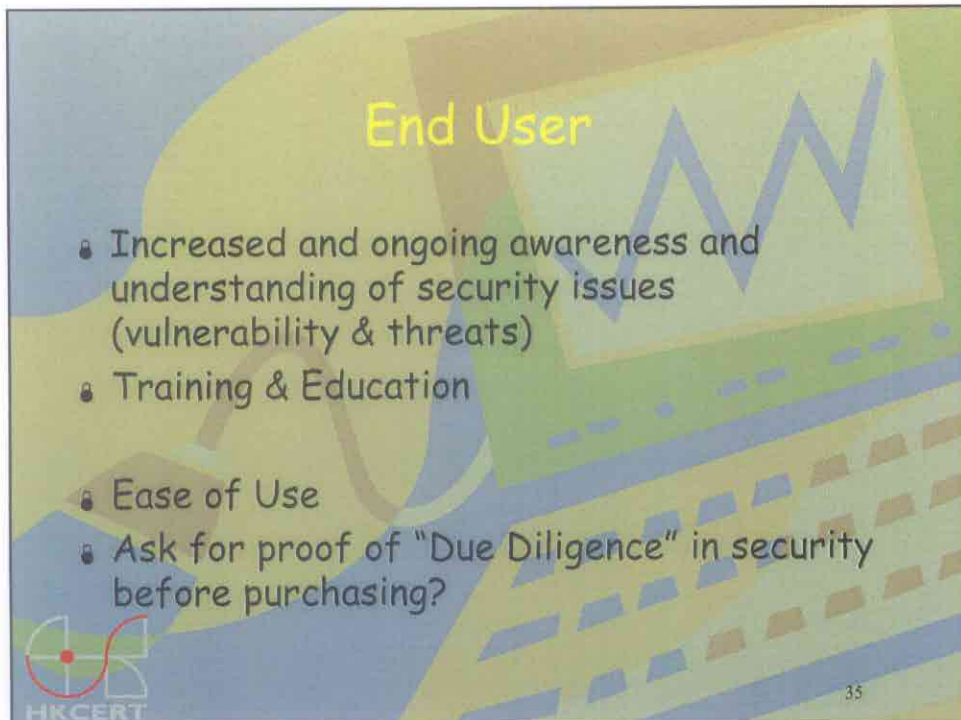
33

Cost of Ownership

- Software Vendors usually disclaim NOT responsible for Errors found in the software
 - Not paying damages
- End Users are bearing the cost of quality
- But, Vendors are spending more effort on Defect Prevention
- End Users will hopefully reduce Total Cost



34

The slide features a background with abstract shapes in shades of blue, green, and yellow. A computer monitor is depicted with a blue line graph showing an upward trend. Below the monitor is a keyboard. The text 'End User' is written in yellow. A list of four bullet points is on the left. The HKCERT logo is in the bottom left, and the number '35' is in the bottom right.

End User

- Increased and ongoing awareness and understanding of security issues (vulnerability & threats)
- Training & Education
- Ease of Use
- Ask for proof of "Due Diligence" in security before purchasing?

HKCERT 35

The slide features the same background as the previous slide. The text 'Thank You' is written in yellow. Below it, the name 'Roy Ko' and email address 'royko@hkcert.org' are written in black. The HKCERT logo is in the bottom left.

Thank You

Roy Ko
royko@hkcert.org

HKCERT