New York e-Commerce Testing

Commercial Practices in IA Testing Panel

22 March 2001
Albuquerque, NM

WINDERMERE

Organization

WINDERMERE

I. Problem Statement
II. Testing Methods
III. The Paper Trail
IV. Ending Notes

I. Problem Statement

WINDERMERE

e-Commerce Environment

- Hurried
- Dynamic
- Aggressive
- Competitive

Typical Startup .com System

WINDERMERE

What do commercial "systems" look like?

- **Hosting Service provides infrastructure and environment**
- **Servers at hosting service run the system applications**
- **Applications are either developed or purchased for integration into system**
- **Testing is often outsourced**

This is different from he typical DoD system

Commercial Attitudes

WINDERMERE

- **Security Requirements are an accepted part of system requirements**
- **Rising Computer Crime is a cause of concern**
  - » Targeting e-Commerce
  - » External & Internal
- **Global Nature of the problem is an issue**
  - » U.S.A.
  - » Korea
  - » Russia
  - » Spain
  - » More…

- **Attackers have a Variety of Purposes**
  - » System Reconnaissance
  - » Denial of Service
  - » Blackmail
  - » Compromise of customer information, credit card accounts, …

"Why do you rob banks?"

"It is where the money is."

Panix

- NYC Internet Service Provider service halted by Denial-of-Service attack
- Newer threats are Distributed Denial-of-Service attacks

Blackmail

WINDERMERE

- Schoolboy Hacker – Caused 20,000 Pounds (Sterling) damage. Tracked easily (source : icnlist)
- CD Universe blackmailed

Credit Card Theft and Database Theft Concerns

WINDERMERE

From:info@bibliofind.com
Date:Mon, 05 Mar 2001 12:03:28 -0500
Subject:Important Information from Bibliofind
To:info2@bibliofind.com

Dear Bibliofind Customer:

Bibliofind has just learned of a security violation on its site that compromised the security of credit card information used on Bibliofind's servers from last October through February 2001. We have no information at this time to suggest that your credit card has been misused, but we wanted to notify you as a precautionary measure. We have been in contact with the federal law enforcement authorities on this matter, and we have also notified the appropriate credit card companies, so that they can take the necessary steps to protect the interests of any cardholders who may be affected. If you have specific questions about your credit card account, please contact the issuer of your credit card. To ensure this doesn't happen again, we have removed all customer credit card information, physical addresses, and phone numbers from Bibliofind's servers. We expect to bring the Bibliofind system back into operation shortly. We apologize for any inconvenience this may cause you. You can contact us with questions at info@bibliofind.com.

Sincerely,

Bibliofind

Trojan Horse

WINDERMERE

From: XXXXX XXXX <XXXXXX@XXXXX.com>

To: “Sam Nitzberg" <snitzberg@witsusa.com>

Subject: Introductions and Inquiry

Date: Fri, 9 Mar 2001 16:27:10 -0500

MIME-Version: 1.0

X-Mailer: Internet Mail Service (5.5.2448.0)

Content-Type: multipart/alternative; boundary="----
_=_NextPart_001_01C0A8DF.B3683BE0"

Sam:

I got your contact information from a colleague of mine. I understand that you are experts in Internet security. I have recently been made aware of a possibility of a Trojan Horse in my production environment. Ideally, I would like to verify its existence, eradicate it, and hopefully capture information of ho wit got there, when, and by whom. I have reason to believe it is an InCommand Access Trojan Horse operating off port 1029.

Is this something you can help us with?

Regards,

XXXXX XXXX

Vice President of Technology

Albuquerque Surrender
(Feb. 2001)

WINDERMERE

Jerome Heckenkamp

- From LANL
- Accused of causing more than $1 M in damage
- Accused of breaking in (or trying to break in) to eBay, Exodus Communications, Juniper Networks, Inc., Etrade, Lycos, Cygnus Support Solutions.

Awareness Sources

WINDERMERE

The New York City E-Commerce Community uses diverse information sources to maintain awareness :

- New York Times
- Wall Street Journal
- MSNBC
- Bloomberg
- More …

Community Meetings

WINDERMERE

ISSA (Information Systems Security Association) NYC Chapter

- **Regular meetings in Manhattan**
- **Presentations**
- **Vendors of security solutions**
- **Regular discussions amongst security professionals**

http://www.nymissa.org

http://www.issa.org

Emergency Contacts

WINDERMERE

- Emergency CERT contact numbers
- Security and Systems Administrators
- FBI contact information
- CIO contact information


II. Testing Perspectives
Many views
WINDERMERE

Types of Security Testing

WINDERMERE

Type of Testing	Description
Risk Assessment	An investigative and analytic process to develop an overall picture of an organization's information protection posture
Security Audit	A formal review of an organization's information systems to verify the implementation and operation of access controls
Vulnerability Scanning	Technical survey of information systems against a set of known vulnerabilities
Stress Testing	Test system transaction capacities including resistance to denial of service attacks
Penetration Testing	Compromise security services and gain unauthorized access to systems or data

"Information assurance" is not a generally used commercial term

Seals of Approval

WINDERMERE

- **Care about :**
  - » Statements that industry practices are being met
  - » Care about government issues
- **Do not care about :**
  - » Specific certifications from security organizations

Related Organizations

WINDERMERE

- **The Financial Services Information Sharing and Analysis Center FS/ISAC for banking, security, insurance industries**
  - » ISAC- A secure database, analytic tools to submit (anonymous or attributed) reports regarding threats, vulnerabilities, incidents, and solutions
  - » No US Government or law enforcement access

http://fsisac.com/fsisac_overview.htm

Forensics

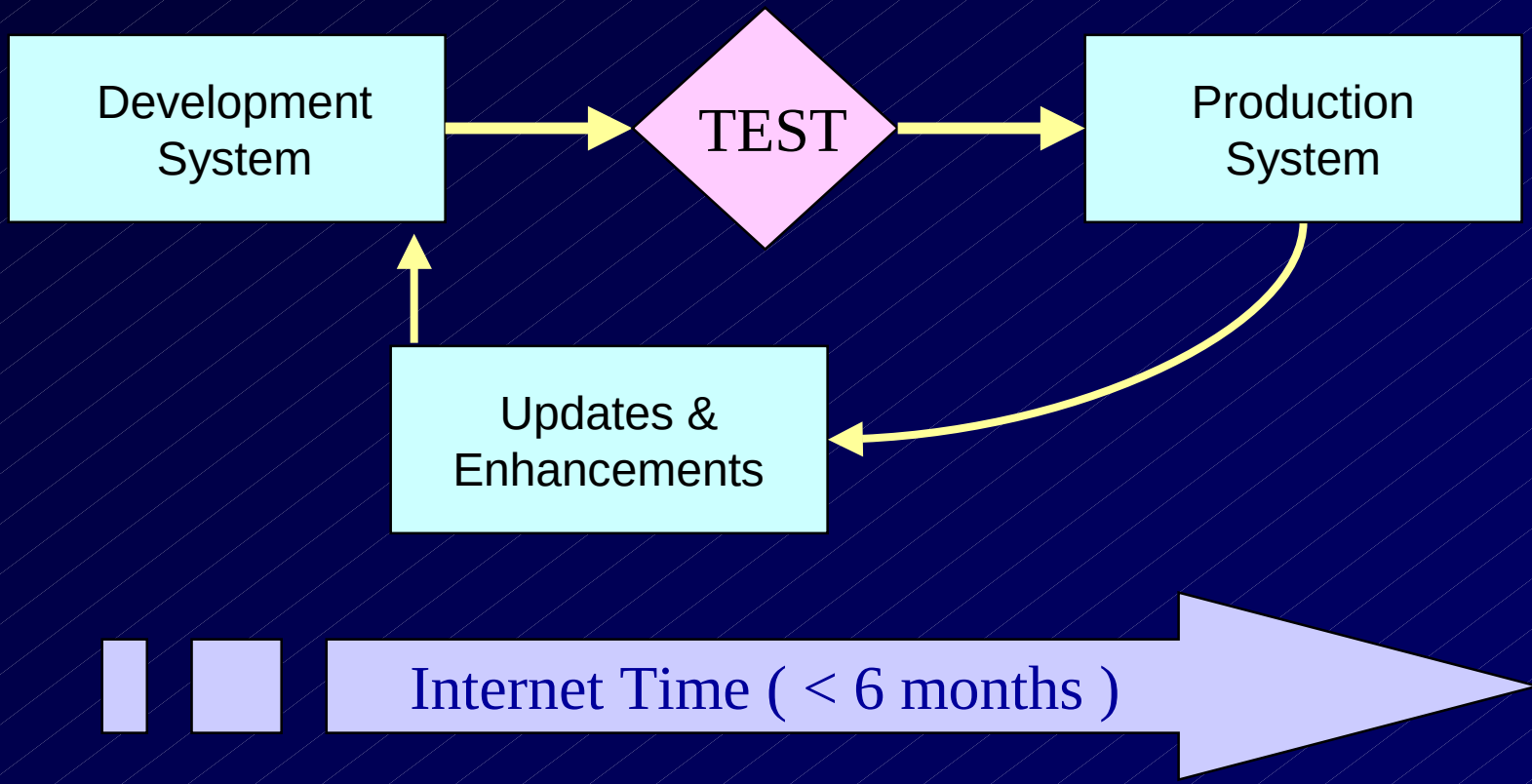
WINDERMERE

- Procedures are in place to properly secure and stow computers and their media in case of detected criminal activity or infiltration
- These procedures must meet legal muster for the handling of evidence
- Recommendation was made to banking and e-commerce representatives to drill for responses to critical incidents

(Ex – FBI Computer Crime Squad office member, NYC

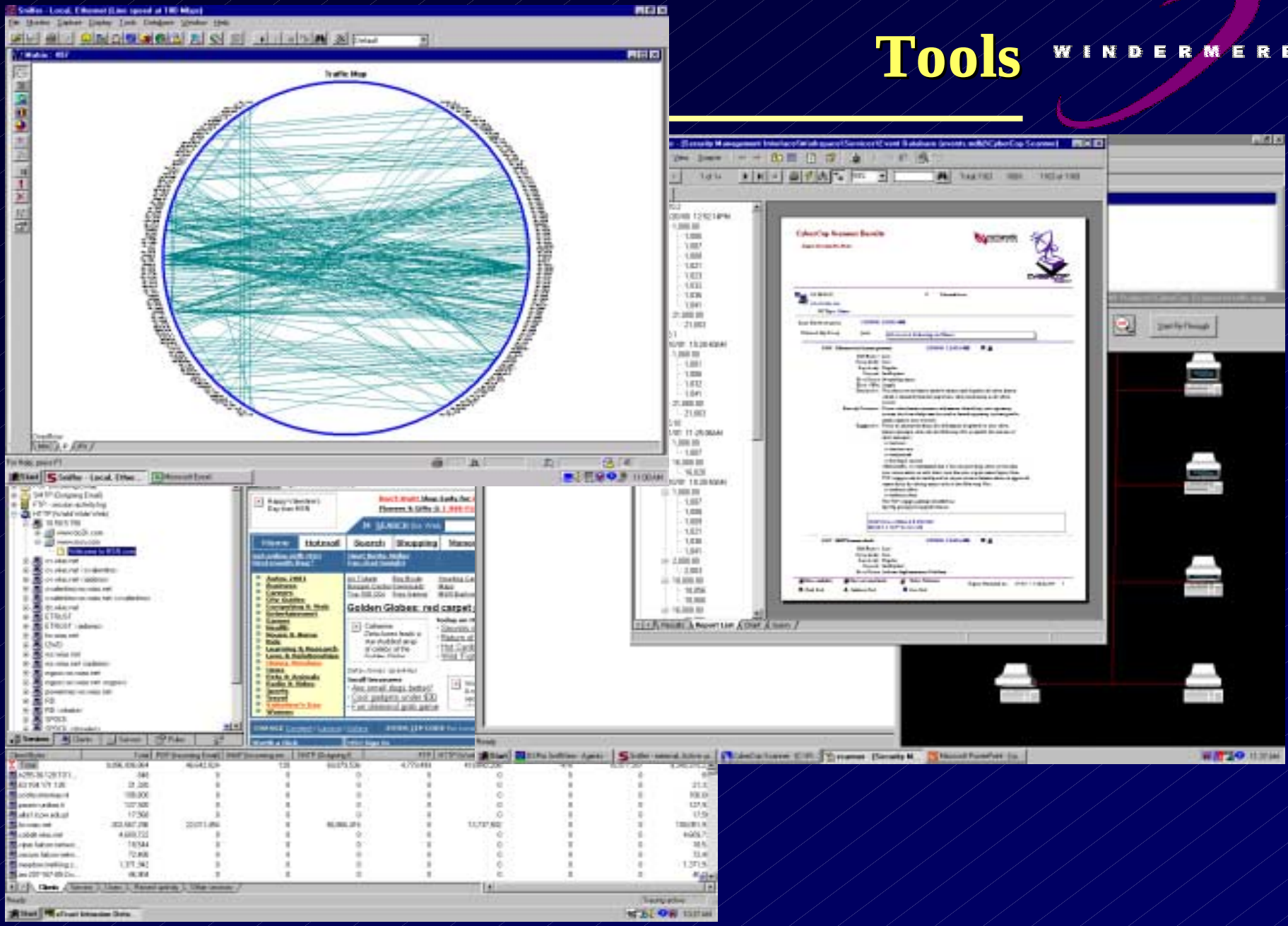
Perspectives and Life-Cycles

WINDERMERE



Tools

WINDERMERE



Production System Protection

WINDERMERE

- **Routine Activities**
  - » Run full-time Denial of service (DOS) checks
  - » Perform Monthly security scans
  - » Perform “Regular” checks of advisories
- **Schedule regular system updates to fix problems or to add enhancements**
  - » Must test and assess systems to ensure that all patches are relevant, current, and do not “break” systems
  - » Not adequately testing patched systems carries risks
  - » Patches may break or impair systems or their security
  - » Over-testing causes delays, prolonging exposure to the security hazards that the patch would repair

Publicly Traded Companies

WINDERMERE

- **All publicly traded groups have independent auditors**
- **External Audit – The "Big Five"**
  - » Provide full audit services including information security
  - » Results go into a consolidated audit report
  - » Main requirements are access controls and accountability
- **The company's internal audit group provides all relevant information:**
  - » Reports from compliance group
  - » Information on networks
  - » Contact information
- **Security Group**
  - » Examines current advisories
  - » Tells groups which tools to put in place
  - » Their guidelines are enterprise-wide
  - » Tracks exceptions to guidelines

III The Paper Trail

What is done with the reports ?

WINDERMERE

Testing Follow-up

WINDERMERE

Once the Test Report is delivered…

- Fixes are made by in-house staff
- Fixes are made judiciously
- Production systems are changed out of cycle only for urgent issues
- Testing is rerun to verify corrections

Results Have High Visibility

WINDERMERE

- Corporate security risks go to security office, CIO,VP and in turn, Chair
- May vary…
- Data will be captured, but what will go up the chain will only be what the executives want
- Some will delegate more security responsibility to a lower level. More critical portals would likely have higher visibility


IV Ending Notes
WINDERMERE

Conclusions

WINDERMERE

- Keep testing as part of the development process even when time is constrained
- Separate the responsibilities for development, test, and verification
- Establish accountability for security
- Maintain current awareness of security issues
- Maintain combination of testing tools
- Test and retest frequently
- Discriminate in analysis of test results
- Implement fixes

Risks

WINDERMERE

- Weighing risks versus costs (“profits”) is a key commerce theme
- In e-commerce, losses are “only money” or “only data”
- Military risks may demand greater risk mitigation

Games of Chance

WINDERMERE

- Banks and e-commerce sites stake their potential losses and their credibility against the success of a damaging security incident
- Those organizations that do not successfully tolerate their threat environment lose: they fail their mission, and they absorb secondary losses through customer attrition

Thank you…..
Questions……..

Sam Nitzberg

snitzberg@witsusa.com

(732) 380-1902

WINDERMERE