Building a Forensics Investigation & e-Discovery Readiness Plan (FIERP)

Inno Eroraha, CISSP, CISM, CISA, CHFI, PI
Founder & Chief Strategist
NetSecurity Corporation

April 28, 2009

netSecurity Forensic Labs

netSecurity

Real-World Scenario:
Pukka Oil Corporation

- Pukka Oil Co, is multi-billion dollar company
- You receive a call from an inside counsel to help with a massive network intrusion/compromise
  - Corporate trade secrets
  - Lists of clients, employees' private information
  - Patent-pending innovations
  - Oil exploration strategies
  - Other proprietary information
- Pukka has not experienced a computer attacks in 49 years of corporate existence – company is stringent in its security measures
- News of the attack are in every new outlets, with executives issuing press conferences
- Cyber criminals are demanding $15 million in ransom to avoid unleashing the corporate loot
- Employees, customers, and partners are filling law suits

Real-World Scenario:
Pukka Oil Corporation (Contd.)

- Cost of the incident requests is $1,200,000 (forensics investigation and e-discovery)
- $28 million in steep fines and punitive damages, resulting in a spiral downward spin of its stock price
- $4.5 billion in total loss in market cap as a result of this incident – Pukka's stock plummeted, with one-half the market valuation dissipated in three months!
- Now investors and shareholders are suing!

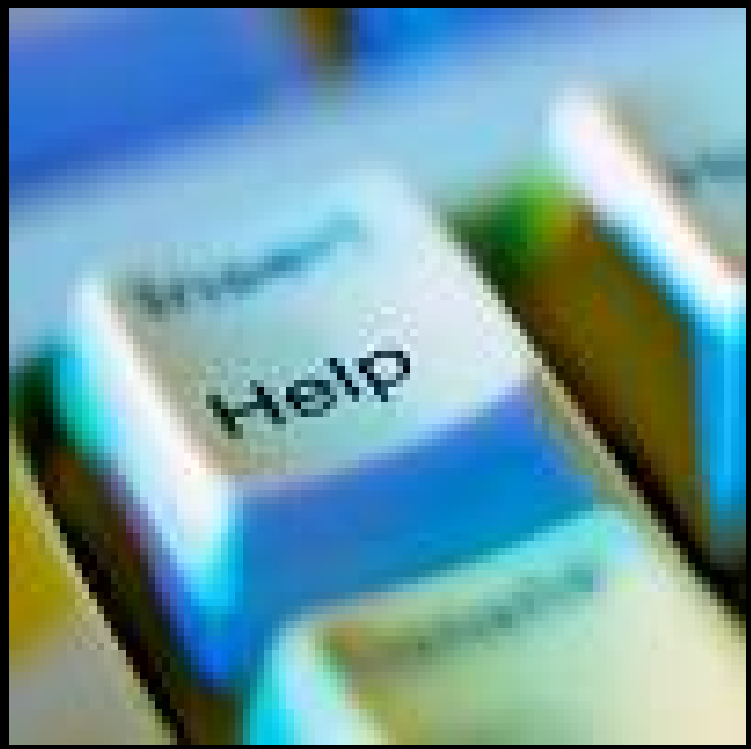
How would You have Minimized the Risk in the Pukka's Scenario?

- (A.) Install more firewalls and security systems
- (B.) Give the executives more perks
- (C.) Quietly pay the ransom to avoid all the bad publicity
- (D.) All of the above
- (E.) None of the above

Presentation Objectives

- **To suggest** ways to reduce business risks that results WHEN forensics investigation or e-discovery requests are warranted
- **To suggest** how-to get an organization ready for forensics investigations and e-discovery requests
- **To suggest** ways of establishing a capability to securely gather legally admissible evidence, respond to and conduct digital investigations, and produce ESI promptly and avoid adverse court rulings

Forensics Investigation and e-Discovery Readiness Plan



The Need for a Readiness Plan

- **Data Ubiquity**
  - Digital information continues to grow at an exponential rate
  - The explosive growth of emerging portable data and storage devices. Information stored in these changing media can be crucial sources of evidence in corporate, civil, and criminal investigations
- **Revised Federal Rules of Civil Procedure (FRCP)**
  - The recent amendments address the discovery of electronically stored information (ESI)
  - Organizations with a viable FIERP are better positioned to quickly and cost-effectively find and produce necessary ESI during investigation
  - Avoid being imposed punitive damages, legal costs, and unfavorable rulings
- **Increase in Cyber Crime against Corporations**
  - Compliance with regulatory requirements (SOX, GLBA, HIPAA, SEC, PCI, etc.)
  - Organizations suffer computer intrusions constantly
  - A well established plan helps the corporation to quickly and better respond to cyber attacks and corporate investigations

Benefits of a FIERP

- A well established plan helps a corporation to quickly and better respond to cyber attacks and corporate investigations
- Help you to establish a capability to securely gather legally admissible evidence
- Helps you to respond to and conduct digital investigations, and produce ESI promptly and avoid adverse court rulings

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Seek Management Buy-in

- Convince them why you think the plan is necessary, the cost, and the impact or penalty for not having one
- Cite recent court rulings where other firms (such as competitors) have been sanctioned or paid huge fines for not responding to e-discovery requests promptly
- With management buy-in, you get the financial resources that are required and gain the support of other managers and employees throughout the enterprise

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Revise Corporate Policies to Address FIERP

- The policy should specify what kind of information would be captured, stored, where, for how long, and why
- The policy should also specify the department that will be responsible for managing digital investigations and e-discovery requests and types of investigations (such as computer abuse, pornography, hacking, and so on) in which the department is to provide support

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Form a Forensic Investigation and e-Discovery Team (FIET)

FIET Members

- Composed of key personnel in from:
  - Legal
  - Human Resources
  - Compliance
  - IT (privacy, record management, disaster recovery, backup team, computer security, incident response, forensics, system administrators, etc.)
- Including members from various parts of the organization provides good insight and information about the location of potentially relevant electronic documents and where digital evidence might reside
- A Manager or should be appointed to lead the team

FIET Members (Contd.)

- Include outside consultants
  - Computer Forensics Experts
  - E-Discovery Consultants
  - Outside Counsels

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Identify or Appoint a FIET Manager ("Czar")

- Responsible for managing and updating FIERP
- Provides central view of corporate information and data
- Should ideally report to senior management (i.e., CEO, CIO, COO, or corporate executive)
- Coordinate with legal and other business units to ensure that digital investigation and e-discovery requirements are incorporated into the business process

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Get a Firm Grip on Your Data

- Corporate data are stored in various devices: computers, Laptops, and hand-held devices
- A thorough knowledge of the data collected or processed by the organization and the storage location of these corporate jewels is an absolute
- Create and maintain a central repository of information

Get a Firm Grip on Your Data

- Create a Repository of Data Custodians and Storage Locations
- Establish a Data Collection and Logging Policy
- Institute a Data Retention Plan and Policy

Get a Firm Grip on Your Data

- **Create a Repository of Data Custodians and Storage Locations**
- **Establish a Data Collection and Logging Policy**
- **Institute a Data Retention Plan and Policy**

Create a Repository of Data

- Data that an organization should include in a repository may be email, spreadsheets, word processing, web transactions, instant messages, database, system log files, and other electronic records
- This data may be stored in email servers, web servers, database servers, employees' desktops, personal laptops, PDA devices, storage area network (SAN), backup tapes, removable media, and off-site (third-parties) storage locations
- For each type of data, the storage location (system and location) and data custodian should be identified and documented
- This repository or inventory can be as complex as a database or as simple as a spreadsheet that is maintained and kept updated by the FIET manager or their designee

Get a Firm Grip on Your Data

- Create a Repository of Data Custodians and Storage Locations
- Establish a Data Collection and Logging Policy
- Institute a Data Retention Plan and Policy

Establish a Data Collection and Logging Policy

- Data logging policy should establish the type of data to store, as may be dictated by business, regulatory, or legal requirements
- Certain system log information may be collected for either root-cause analysis, after-the fact forensics investigation, or live incident response event
- Determine the type of data to gather and collect voraciously
- The critical nature of a system or information might determine the amount of data to collect, store, and archive
- Computer incident investigations may be easily accomplished if there is reasonable data to analyze for evidence of a malicious activity or other compromises

Get a Firm Grip on Your Data

- **Create a Repository of Data Custodians and Storage Locations**
- **Establish a Data Collection and Logging Policy**
- **Institute a Data Retention Plan and Policy**

Institute a Data Retention Plan and Policy

- Data retention policies address the need to maintain information in an organization's possession for a period of time, depending on the type of data and the business, legal, or regulatory requirements
- Clear written policies and procedures should be developed, taking into account procedures that address the creation, retention, retrieval, archival, and destruction of the information at stake
- Retention policy should spell out how long certain information and data are to be archived or destroyed, based upon the type of data
- Record retention policy should be widely communicated, easily accessible, easily understood by employees, and simple to follow
- Policies and procedures should include the suspension of destruction of information, which may be required to comply with preservation requests, pending litigation, or ongoing investigation

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Build and Equip a Forensics Investigation Lab

- Obtain a Facility to Conduct Investigation
- Acquire Investigative Tools and Technologies for the Lab
- Test and Validate the Tools
- Train the Investigation and e-Discovery Team

Build and Equip a Forensics Investigation Lab

- **Obtain a Facility to Conduct Investigation**
- **Acquire Investigative Tools and Technologies for the Lab**
- **Test and Validate the Tools**
- **Train the Investigation and e-Discovery Team**

Forensics Investigation Lab

Obtain a Facility to Conduct Investigation

- A critical part of the FIERP is to include a lab environment where investigations can be conducted -- CO$T should be a factor
- Lab may be an entire building or part of a building that is sectioned off and secured, strong access control, and entry granted on a need-to-know basis
- The lab should be built with specific requirements and minimum equipment and tools that can be used to collect, analyze, produce, or archive digital evidence
- There should be ample ventilation, humidity control, air-conditioning, and reliable electric and power supply
- Areas with computers or electronic components must be well grounded to avoid static electricity that may damage hard drives or computing devices

Build and Equip a Forensics Investigation Lab

- Obtain a Facility to Conduct Investigation
- **Acquire Investigative Tools and Technologies for the Lab**
- Test and Validate the Tools
- Train the Investigation and e-Discovery Team

Acquire Investigative Tools & Technologies for the Lab

- Tools to include should support mainframe computers, Unix, Windows, and MAC OS, or other applicable platforms
- Select investigative tools should include: handheld device forensics equipment; computer forensics software and hardware, including: acquisition (imaging, duplicating, copying), analysis, write-blockers, image mounting, drive erasure, archival, and assorted accessories
- Tool arsenals should include specialized ones, such as those that perform specific actions: steganography analyzers, decryption software, and live data collection and incident response tools
- Specialized e-discovery tools for searching, indexing, restoring, migrating, analyzing, and reporting should be purchased for the lab
- Technologies to consider include networking equipments, analysis workstations, and storage area network (SAN) to store massive enterprise data

Build and Equip a Forensics Investigation Lab

- Obtain a Facility to Conduct Investigation
- Acquire Investigative Tools and Technologies for the Lab
- **Test and Validate the Tools**
- Train the Investigation and e-Discovery Team

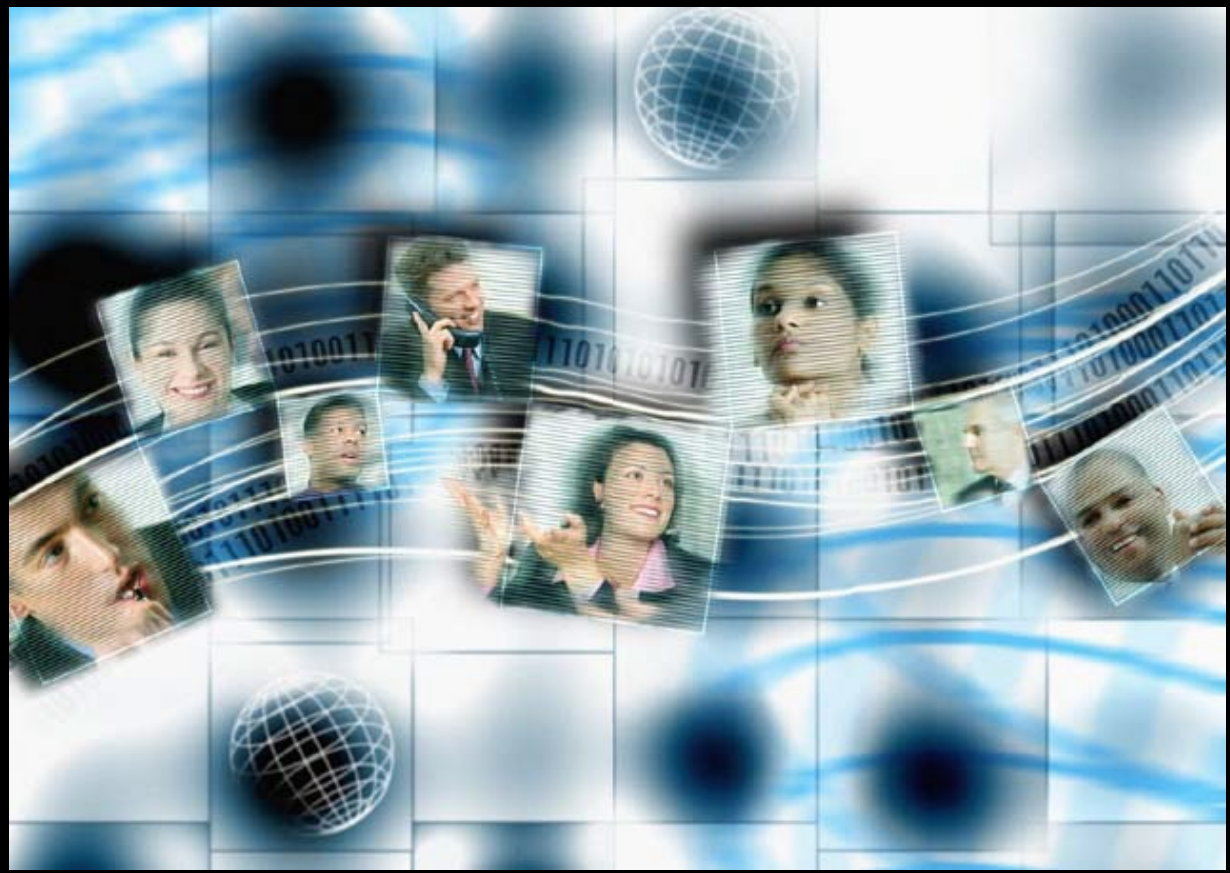
Test and Validate the Tools

- Before the purchase of investigative tools, they should be tested to ensure that they work in the target environment
- Tools should be validated to ensure that technologies used for collection, investigation, and analysis maintain data integrity before an actual investigation occurs

Build and Equip a Forensics Investigation Lab

- Obtain a Facility to Conduct Investigation
- Acquire Investigative Tools and Technologies for the Lab
- Test and Validate the Tools
- Train the Investigation and e-Discovery Team

Train the Investigation and e-Discovery Team



Train the Investigation and e-Discovery Team

- Employees that are responsible for collecting, processing, and analyzing evidence should be trained continuously, especially on how to collect certain type of evidence or on new ways of investigating emerging attacks or hacking techniques
- A hands-on training provides the skills needed by these personnel to handle necessary tasks in a real-world or simulated scenarios
- Training should include: forensics, incident response, e-discovery, evidence handling, chain of custody, testifying in courts, and how to use the tools and technologies that have been purchased for investigation

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Create Standard Operating Procedures (SOPs)

- SOPs define the procedures that employees are to follow in order to carry out a specific investigative tasks ensuring that errors are minimized and procedures have been followed
- SOP should describe the procedures for conducting forensics investigation and e-discovery request in a manner that avoids questioning the methodology applied on a particular investigation or e-discovery request
- The standard operating procedure should define a forensic imaging process, which spells out the process to implement for ensuring forensics soundness of digital evidence
- SOP should include a process for collecting or producing electronic evidence; a process to follow when discovery requests have been received; a plan for litigation hold requests; a process for securing and handling of evidence; and a process to identify available sources and types of evidence
- SOP should describe the training requirement and skills of the investigators, incident responders, data collectors, and analysts

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Test and Rehearse the Plan

- The only way you gauge if your plan is working is to actually test it before it is used in a real-world scenario
- Testing results in updates to the plan, continuous awareness of latest amendments to FRCP, and best practices for preparing for e-discovery requests and conducting forensics investigations
- Testing ensures that the plan is working as planned and supports the organization should the need to conduct an investigation or fulfill an e-discovery request arises
- Creating real-world scenarios for e-discovery request, litigation holds, or computer hacking is suggested to demonstrate how the organization can conduct investigations and test employees in the awareness of the FIERP
- Depending on the scope or goals of the testing, few employees or participants, or even the entire corporation may be notified of the testing and rehearsal
- The results of the testing and rehearsal exercise should be documented in an after-action report, which should be considered and used in updating the FIERP

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Conduct FIERP Awareness Campaign & Training

- A well developed plan will serve no useful purpose unless it is clearly communicated to stakeholders, employees, or parties to whom the plan applies
- An awareness campaign and training should be done regularly
- Employees should receive training on incident recognition, awareness, laws, and their roles in ensuring that the organization implements the FIERP and cooperate with investigation

The Human Element: Training Employees

- Identify data they should be storing
- Define company rules for handling and storing sensitive information
- Train on incident awareness and recognition
- Outline consequences for violating company policies/procedures
- Retrain on a regular basis

Building a Forensic Investigation and e-Discovery Readiness Plan

- Seek Management Buy-in
- Revise Corporate Policies to Address Forensics Investigation and e-Discovery Planning
- Form a Forensics Investigation and e-Discovery Team (FIET)
- Identify or Appoint a FIET Manager
- Get a Firm Grip on Your Data
- Build and Equip a Forensics Investigation Lab
- Create a Standard Operating Procedure (SOP)
- Test and Rehearse the Plan
- Conduct FIERP Awareness Campaign & Training
- Update the FIERP

Update the FIERP

- Updating is critical to the viability of the FIERP
- Updating involves taking the output and documented results from the testing and rehearsal stage or plan review feedback to revise the plan and make it more up to date based on latest amendments to FRCP and new unforeseen threats

THE FIERP IS A "LIVING" DOCUMENT

Conclusion

- The efforts spent putting together a FIERP would help your organization save costs, avoid steep fines or other adverse court rulings
- To comply with regulatory and legal requirements and investigate cyber crimes promptly, corporations should institute a forensics investigation and e-discovery readiness plan
- Senior management should provide buy-in, policies should be developed, and the organization should have a firm grip of its data
- A response capability should include securing a lab environment, equipped with tools and technologies for carrying out investigations and e-discovery requests
- FIERP must be tested frequently and updated accordingly

Selected References

- *Federal Rules of Civil Procedure,* http://www.law.cornell.edu/rules/frcp/
- *Amendments to the Federal Rules of Civil Procedure,* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf
- *Techno Security's Guide to E-Discovery and Digital Forensics*, Jack Wiles, et al.
- *Handbook for Computer Security Incident Response Teams*, http://www.cert.org/archive/pdf/csirt-handbook.pdf
- *Building a Computer Forensics Lab*, http://computerforensicslab.blogspot.com/
- *Creating a Computer Security Incident Response Team: A Process for Getting Started,* http://www.cert.org/csirts/Creating-A-CSIRT.html
- *Avoiding the Trial-by-Fire Approach to Security Incidents,* http://www.sei.cmu.edu/news-at-sei/columns/security_matters/1999/mar/security_matters.htm

Thought Provoking Discussion/Scenarios

netSecurity Forensic Labs

netSecurity®

Direct Comments/Questions to:

Inno@NetSecurity.com

netSecurity Forensic Labs

netSecurity®