Organizational Issues of Implementing Intrusion Detection Systems (IDS)

Shayne Pitcock, CISSP

First Data Corporation

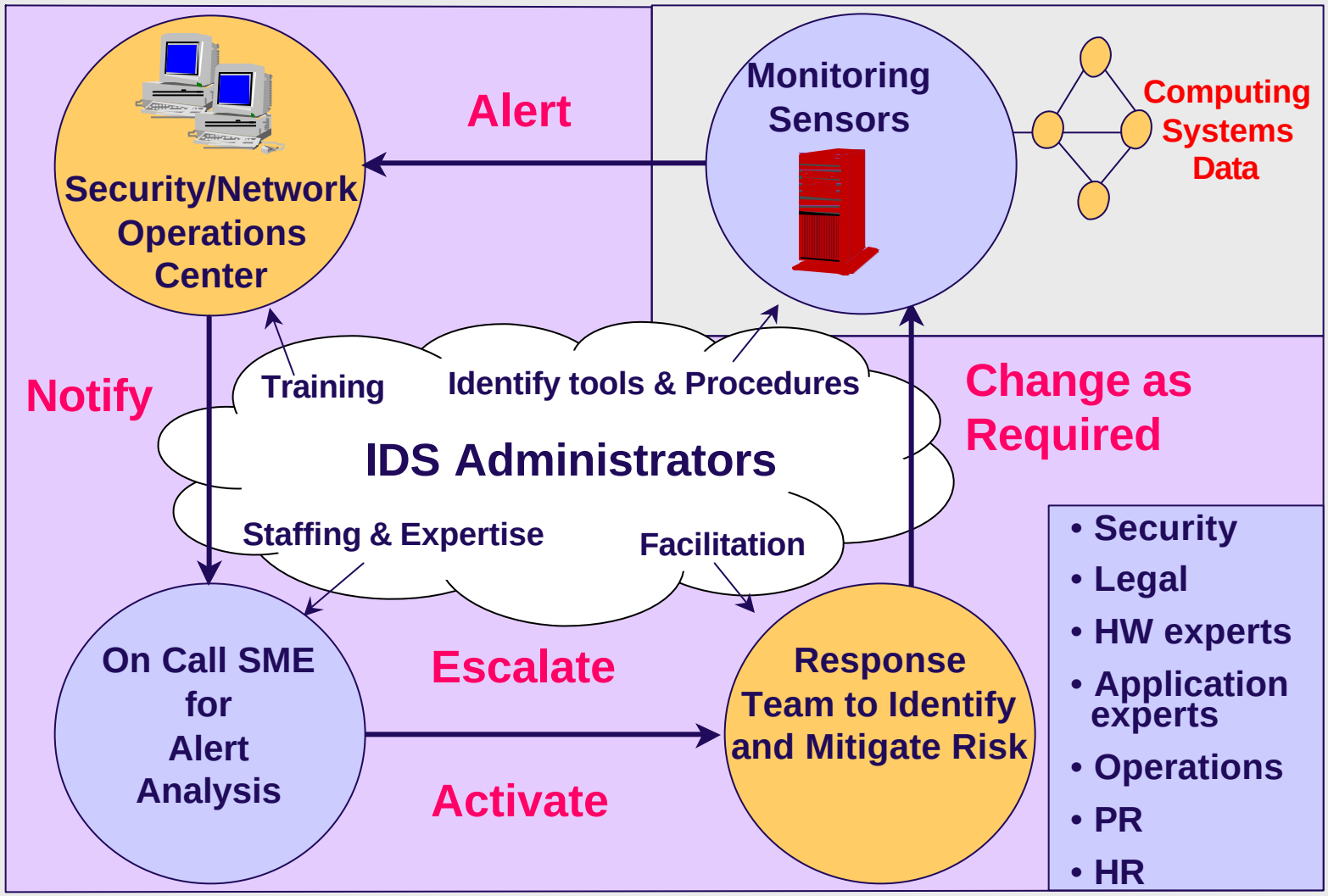
NEbraskaCERT

Agenda

- Problem Description
- Issues for Consideration
- Mitigation of the Issues
- Options for Implementation of IDS Tools
- Quantifiable Metrics
- Conclusion

NEbraskaCERT

Problem Description



NEbraskaCERT

Issues for Consideration

- Security Policy Development
- Business Requirements for Using IDS
- Impacts to Computing Environment
- Security Alerts
  - Integration and Management
  - Resolution
  - Incident Response

NEbraskaCERT

Security Policy Development

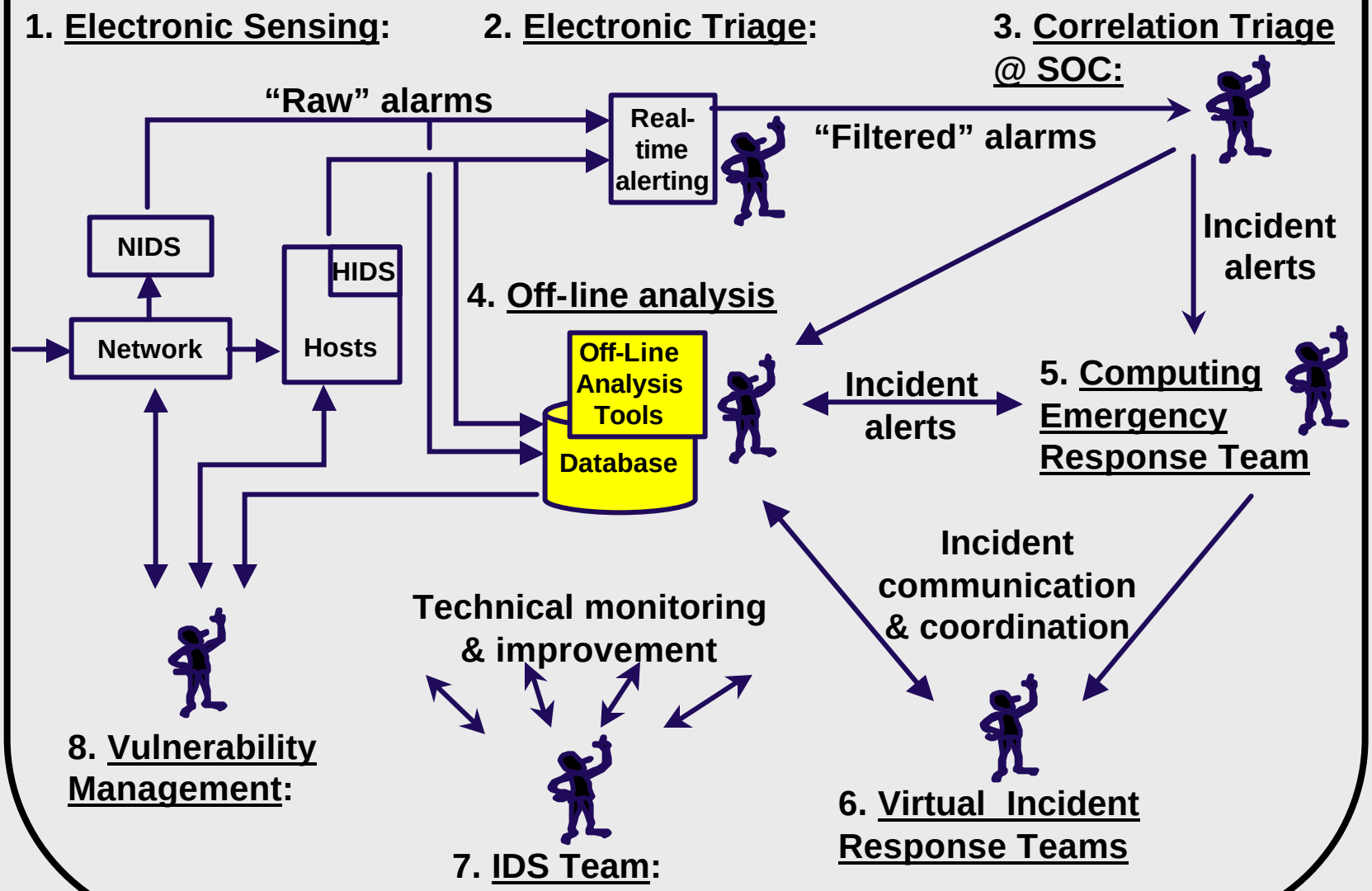
- Establishes corporate level need for IDS
  - Approval
  - Guidance
  - Direction
- Establishes responsible organization for implementation and control of the IDS tools
- Establishes expected output of the IDS implementation
  - Reports
  - Incident Response
  - Attack Mitigation

NEbraskaCERT

Business Requirements for IDS

- Federal mandate by GLBA and HIPAA
- Business partner connections
- Distributed business units within the company
- Specialized security alerting and analysis of “suspicious” activity

Impacts to Computing Environment



NEbraskaCERT

Alert Integration and Mgt.

- Consolidating security alerts from multiple sources (firewalls, IDS, and network gear)
- Actively monitoring and responding to all alerts
- Managing the volume of security alerts
- Normalizing the alert data for common points of integration

NEbraskaCERT

Alert Resolution

- Correlating the various alerts from multiple security sources
- Evaluating the risk of “suspicious” activity
  - Determining the level of vulnerability
  - Determining what is within “normal” activity for the monitored environment
- Mitigating false positive alerts
- Communications with security, network, or operating system (OS) administrators
- Documentation

NEbraskaCERT

Alert Incident Response

NEbraskaCERT

Mitigation of the Issues - Program Management Approach

- Define
- Plan
- Fund
- Implement
- Test
- Deliver
- Maintain

NEbraskaCERT

Mitigation of the Issues - System Engineering Approach

- Define the requirements
- System design
- Build the pieces
- Test the pieces
- Integration testing
- System delivery
- Maintenance

NEbraskaCERT

Options for IDS Implementation

- Company Resources
- Out-Sourcing to Consultants or Managed Security Service Providers
- Utilizing Vendor Professional Services

NEbraskaCERT

Use Company Resources When…

- Top Secret or Highly Sensitive Information (e.g. military, financial, or international).
- Company is diversified across geographical continents.
- Company has appropriate staff to support the implementation.
- Company is diversified across multiple business disciplines. An example is a company with both Government and Commercial business customers.

NEbraskaCERT

Use Out-Sourcing When…

- Consultants
  - Temporary addition to current staff
  - Expertise beyond the current level of staff
  - “Jump-Start” for an IDS deployment or alert monitoring operations
- Managed Security Service Providers
  - 24 x 7 x 52 alert monitoring operations staff
  - Alert consolidation and correlation
  - Expertise for risk awareness and analysis
  - False positive mitigation
  - Alert resolution and incident escalation

NEbraskaCERT

Use Vendor Services When…

- Single vendor approach to deployment of IDS tools.
- Single vendor providing a majority of the computing systems used by the company.
- To augment the expertise of company personnel.
- To provide indirect training of the product during implementation.

NEbraskaCERT

Quantifiable Metrics

- Reports
  - Actions grouped according to company risk
    - “Suspicious” Activity
    - Attempted Intrusion
    - Escalated Events
    - Incidents for Resolution
  - Top 10 “suspicious” IP addresses
  - Numbers of high, medium, and low alerts
- System status of IDS tools

NEbraskaCERT

Conclusion

- IDS tools are good for specialized security alerting and analysis of “suspicious” activity.
- Implementing an IDS solution requires that a company address how they will monitor and resolve the associated alerts.
- Considerations for the 80% of the solution will greatly enhance the security posture.