Logging And Alerting

Thursday, September 20, 2012

2:15 PM to 3:00 PM

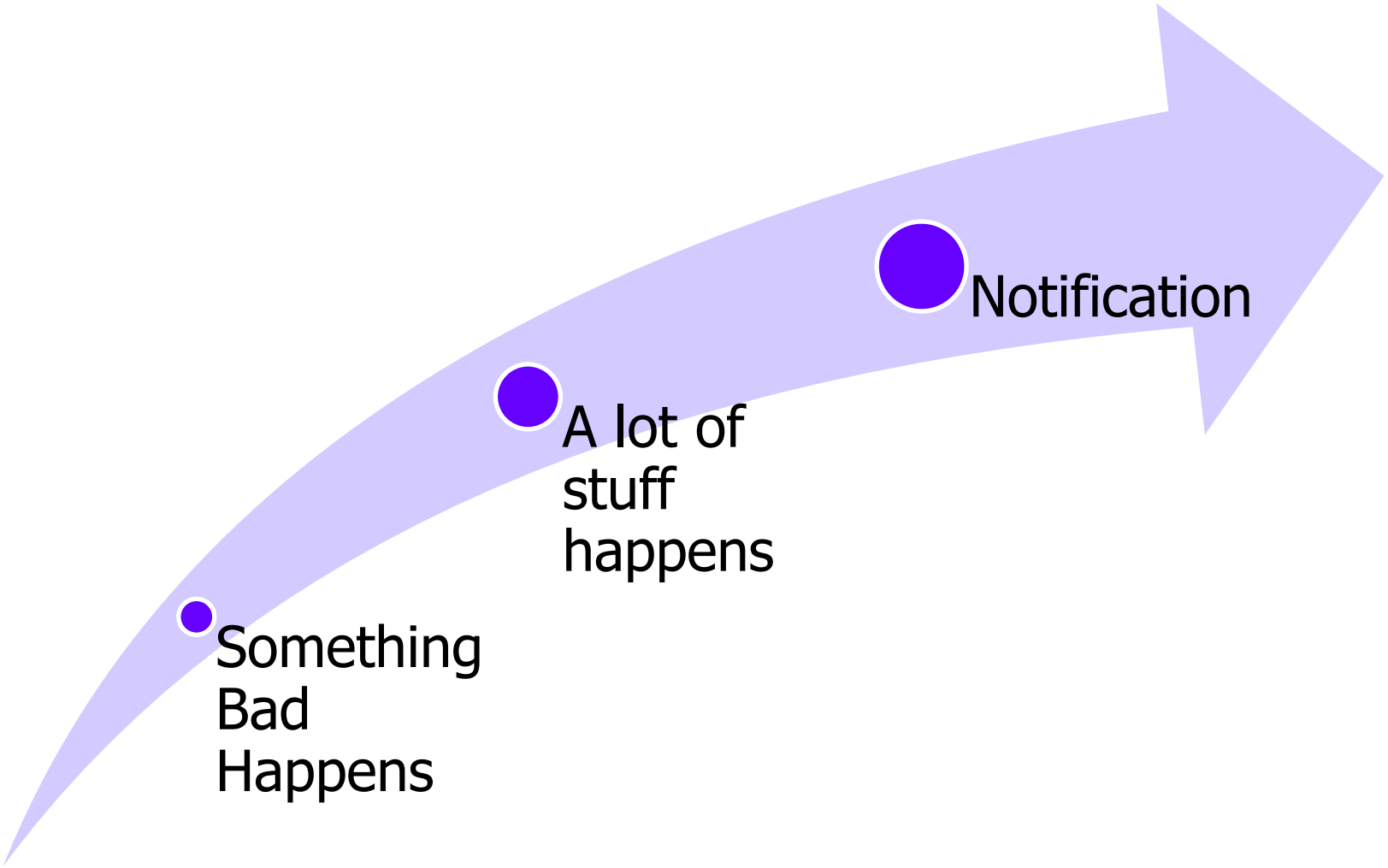
George G. McBride

Director, IT Risk Management Johnson & Johnson

IT Governance, Risk & Compliance

MIS TRAINING INSTITUTE

Logging and Alerting



Introduction. What is log management?

- Collection, storage, and analysis of security log files from multiple systems.
  - Devices, servers, systems, mobile devices, etc.
- Alerting is the process of notifying some process or person that a specific event that has occurred.
  - Event may be known (signature) or unknown (behavior based).
  - Must not de-sensitize the organization through false-positives
- Component of an organization's risk management program, investigations, and compliance teams

Logging And Alerting Program

- Charter
- Organization
  - Staffing models. Qualifications. Job Requirements.
- Roles & Responsibilities
  - Detailed descriptions of the various roles
- Interfaces
  - Communications with other organizations / functions
- Documented Procedures
- Auditing

Logging Basics:

- What device types are in your infrastructure?
- What does the network look like:
  - Logging By Location:
    - DMZ? Extranet?
- Commercial Solution vs. Organic
  - Many successful solutions are mixed / heterogeneous
  - Interfaces /translators are often customized (and the source of failures)
- Can be outsourced or off-shored

Before You Continue….

- Why you are logging?
  - Protect Assets
  - Compliance to regulatory requirements
  - Industry Standards / Best Practices
  - Investigations and forensics
  - Reduce Risk
- Build the right program!

Regulatory Requirements

- Health Insurance Portability And Accountability Act
  - NIST Publication 800-66 provides guidance on what to log.
  - Regulation includes provisions around physical protection of the logs, masking of Protected Health Information (PHI)
- PCI Data Security Standards
  - Adequate logging that includes logged event types and details
  - Log retention of 1 Year. 3 months easily accessible.
  - Central log aggregation in a controlled environment.
  - Log protection and security including log access and data integrity control.
  - Daily log review which can be completed automatically

Regulatory Requirements

- Sarbanes Oxley (SOX) Act
  - Used to identify security violations and exploitation
  - For auditors to review as part of their program to review logs and audits of logs
- Federal Information Security Management Act (FISMA)
  - Reference NIST SP 800-53, Recommended Security Controls for Federal Information Systems
  - Describes log management controls including the generation, review, protection, and retention of audit records and logging data

Considerations:

- Bandwidth:
  - Not all networks are created equal
  - You won't be the first person who takes a network down due to logging issues!
- Capacity:
  - Storage is cheap, but still not free. Or unlimited.
- Why are you logging:
  - Helps define collection, retention, and analysis

Log Management Architecture

Log Generation

- Multiple Source Devices
- Network Collectors / Taps
- Hosts / Networks / Systems

Analysis & Storage

- Accept log data in real-time or batch
- Aggregate and analyze logs
- Transfer to storage devices

Monitoring & Reporting

- Presents in a human readable format
- Used to monitor and review log data
- Used by reporting engines

Log Storage

- Pre-Filtering
  - Reduction of what is stored – some loss of fidelity
  - May eliminate part of the data packets
- Tiered Storage:
  - Hierarchical Storage Management
    - HSM manages storage of data – balances between cost and performance.
- On-Line vs. Off-Line – What is needed "now" versus what can be restored and available.
  - What are the availability expectations?

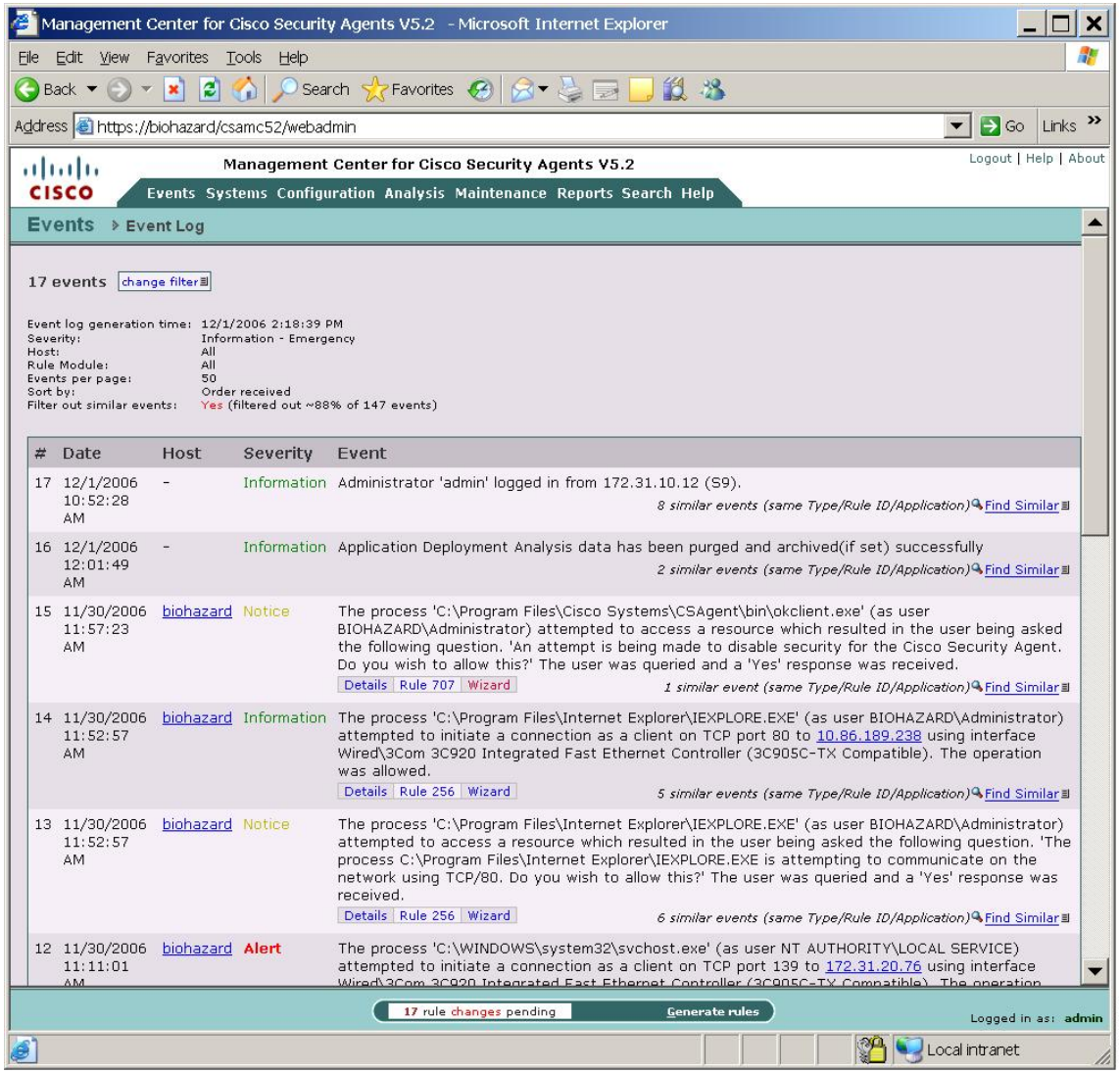
Log Storage

- What happens when you run out of room?
  - Should be alerting well prior to this occurring!
  - Delete older first
  - Remove meta-data (lighten the load)
  - Stop storing new data
  - Mark certain log segments as "Do not delete"
  - How to manage older data that is part of an ongoing investigation
  - Auto-archive?

Log Security

- Secure the overall process
- Secure the transmission
  - Remember: Confidentiality, Integrity, and Availability
- Data Protection
  - Integrity Checks Through Secure Hash Functions
- Access Control
  - Who can access the data?
- Audit Logs of The Log
  - Log changes to the data and by whom

Log Display: Aggregated vs. Raw




```
./q -l 1028 192.168.2.128
...+++++
.............................+++++
[connected to 192.168.2.128:1028]

22:07:46.948617 192.168.2.130.32917 > 192.168.2.128.1028: S [tcp sum ok]
354037143:354037143(0) win 5840 <mss 1460,sackOK,timestamp 6202934 0,nop,wscale 0> (DF)
(ttl 64, id 35745, len 60)
22:07:46.952743 192.168.2.128.1028 > 192.168.2.130.32917: S [tcp sum ok]
3364650016:3364650016(0) ack 354037144 win 5792 <mss 1460,sackOK,timestamp 1188874
6202934,nop,wscale 0> (DF) (ttl 64, id 0, len 60)
22:07:47.051268 0:50:56:f2:ed:f9 0:50:56:eb:22:77 0800 66: 192.168.2.130.32917 >
192.168.2.128.1028: . [tcp sum ok] 1:1(0) ack 1 win 5840 <nop,nop,timestamp 6202935
1188874> (DF) (ttl 64, id 35746, len 52)
22:07:47.051314 192.168.2.130.32917 > 192.168.2.128.1028: P [tcp sum ok] 1:537(536) ack 1
win 5840 <nop,nop,timestamp 6202936 1188874> (DF) (ttl 64, id 35747, len 588)
0x0000   4500 024c 8ba3 4000 4006 26b6 c0a8 0282        E..L..@.@.&.....
0x0010   c0a8 0280 8095 0404 151a 2d98 c88c 7c21        ..........-...|!
0x0020   8018 16d0 ba6c 0000 0101 080a 005e a638        .....l.......^.8
0x0030   0012 240a 8000 0000 8000 0000 8000 0000        ..$.............
0x0040   0000 0000 0000 0000 0000 0000 3322 7f95        ............3"..
0x0050   16b7 0cdf c696 a626 a843 5462 4b55 0f50        .......&.CTbKU.P
0x0060   2d8f 14e6 855b ac0e 171c 1428 91e7 d613        -....[.....(....
0x0070   220d 94f5 6705 cc36 f5ff 4b3e 67a1 8129        "...g..6..K>g..)
0x0080   7a8b 59c5 f8c4 189b a27b 8387 64a4 eb6d        z.Y......{..d..m
<snipped for brevity>
0x0240   cac6 a443 f9b2 df0a be8c 6596                   ...C......e.
22:07:47.026028 192.168.2.128.1028 > 192.168.2.130.32917: P [tcp sum ok] 1:537(536) ack
537 win 6432 <nop,nop,timestamp 1188875 6202936> (DF) (ttl 64, id 22572, len 588)
0x0000   4500 024c 582c 4000 4006 5a2d c0a8 0280        E..LX,@.@.Z-....
0x0010   c0a8 0282 0404 8095 c88c 7c21 151a 2fb0        ..........|!../.
0x0020   8018 1920 e11a 0000 0101 080a 0012 240b        ..............$.
0x0030   005e a638 8000 0000 8000 0000 8000 0000        .^.8............
0x0040   0000 0000 0000 0000 0000 0000 d742 f293        ..............B..
0x0050   c790 d5bb 9927 2c88 8fda f040 4e9b d178        .....',....@N..x
0x0060   d72e 7d58 453f fb38 42f0 9226 db33 3f1a        ..}XE?.8B..&.3?.
0x0070   98aa b49c 6d77 091d c3ed 20b6 eab8 f9c4        ....mw..........
0x0080   268d 8df3 e1b9 97c0 03c0 95e1 409c 4633        &...........@.F3
<snipped for brevity>
0x0240   6540 7718 fce2 2679 ed5b 1fa4                   e@w...&y.[..
22:07:47.027458 192.168.2.130.32917 > 192.168.2.128.1028: . [tcp sum ok] 537:537(0) ack
537 win 6432 <nop,nop,timestamp 6202939 1188875> (DF) (ttl 64, id 35748, len 52)
22:07:47.027480 192.168.2.130.32917 > 192.168.2.128.1028: P [tcp sum ok] 537:565(28) ack
537 win 6432 <nop,nop,timestamp 6202939 1188875> (DF) (ttl 64, id 35749, len 80)
0x0000   4500 0050 8ba5 4000 4006 28b0 c0a8 0282        E..P..@.@.(.....
0x0010   c0a8 0280 8095 0404 151a 2fb0 c88c 7e39        ........../...~9
0x0020   8018 1920 e845 0000 0101 080a 005e a63b        .....E.......^.;
0x0030   0012 240b 0100 0000 0100 0000 0100 0000        ..$.............
0x0040   0000 0000 0000 0000 0000 0000 1100 0000        ................
22:07:47.028364 192.168.2.128.1028 > 192.168.2.130.32917: P [tcp sum ok] 537:565(28) ack
565 win 6432 <nop,nop,timestamp 1188875 6202939> (DF) (ttl 64, id 22573, len 80)
0x0000   4500 0050 582d 4000 4006 5c28 c0a8 0280        E..PX-@.@.\(....
0x0010   c0a8 0282 0404 8095 c88c 7e39 151a 2fcc        ..........~9../.
0x0020   8018 1920 e829 0000 0101 080a 0012 240b        .....).........$.
0x0030   005e a63b 0100 0000 0100 0000 0100 0000        .^.;............
0x0040   0000 0000 0000 0000 0000 0000 1100 0000        ................
22:07:47.041642 192.168.2.130.32917 > 192.168.2.128.1028: P [tcp sum ok] 565:1613(1048)
ack 565 win 6432 <nop,nop,timestamp 6202940 1188875> (DF) (ttl 64, id 35750, len 1100)
0x0000   4500 044c 8ba6 4000 4006 24b3 c0a8 0282        E..L..@.@.$.....
0x0010   c0a8 0280 8095 0404 151a 2fcc c88c 7e55        ........../...~U
0x0020   8018 1920 067e 0000 0101 080a 005e a63c        .....~.......^.<
0x0030   0012 240b 0001 0000 0001 0000 8000 0000        ..$.............
0x0040   0000 0000 0000 0000 0000 0000 08be c71f        ................
<snipped for brevity>
0x0440   fb24 e6b2 84cd 0e53 519c b383                   .$.....SQ...
22:07:50.392850 0:50:56:eb:22:77 0:50:56:f2:ed:f9 0800 110: 192.168.2.128.1028 >
192.168.2.130.32917: P [tcp sum ok] 565:609(44) ack 1613 win 8384 <nop,nop,timestamp
1189218 6202940> (DF) (ttl 64, id 22575, len 96)
0x0000   4500 0060 582f 4000 4006 5c16 c0a8 0280        E..`X/@.@.\.....
0x0010   c0a8 0282 0404 8095 c88c 7e55 151a 33e4        ..........~U..3.
0x0020   8018 20c0 6bc5 0000 0101 080a 0012 2562        ....k.........%b
0x0030   005e a63c 0500 0000 0500 0000 0500 0000        .^.<............
0x0040   0000 0000 0000 0000 0000 0000 1a79             .............y
0x0050   c989 4bbe 6712 c9ae d047 05e4 74cb c8ae        ..K.g....G..t...
22:07:50.399953 192.168.2.130.32917 > 192.168.2.128.1028: . [tcp sum ok] 1613:1613(0) ack
609 win 6432 <nop,nop,timestamp 6203312 1189218> (DF) (ttl 64, id 35751, len 52)
```

Alerting

- Typical organization logs hundreds of thousands to millions of events per day.
  - What matters to organizations. What types of events do you want to know about.
  - False positives? Really?
  - Tuning is continuous. It is NOT a start-up phase.
- Understand what the output of an Alert is:
  - Notification for further review by an Analyst
  - Creation of a trouble ticket
  - Initiate an investigation

Security Event Log Management

- Also known as Security Information Event Management
- Includes:
  - **Data Aggregation:** consolidate monitored data to help avoid missing crucial events.
  - **Correlation:** looks for common attributes and trends and aggregates events over multiple time spans together into cohesive packages
  - **Alerting:** the automated analysis of correlated events and generation of some type of alert
  - **Dashboards:** Tools to report on the data including reporting, informational screens, metrics.
  - **Compliance:** automatically create reports that adapt to existing security, governance and auditing processes
  - **Archiving:** Employ longer term storage of historical data to facilitate correlation of data over time both on-line and off-line

Log File Rotation

- Closes the current log file and creates a new log file
  - Based on size, number of events captured, time in days or hours
- Helps compartmentalize data for data integrity and data management
- Rotated log files can be reduced in size through:
  - Compression
  - Deletion of extraneous information
- Can be easily shared, stored, transmitted

Log Archiving

- Storage of logs for an extended period of time
  - "Extended" is open to interpretation.
    - Sometimes its anything outside of the logging system.
- Archival may be:
  - Off-Line: Accessible, but typically requires intervention to access.
  - On-Line: Typically available in near real-time.
- Log Preservation: retaining logs typically discarded for a specific purpose such as an investigation
- Watch regulatory requirements to ensure compliance

Log Retention

Virtually every organization retains all data ever collected

- The only caveat is when they run out of room and can't acquire more, they arbitrarily delete older data.
- Data Retention Policy – What is it?
- Data Retention Schedule – Different for different types?
- Should have provision for investigations / incident tracking so that data retention may be
- Validating Data Disposal at all collection, storage, processing, transmission points
- Automate the destruction process

Passive Testing

- Doesn't introduce packets or data into the network
- Includes a review of:
  - Policies, Practices, Standards, Procedures
  - Data flows
  - Data Retention
  - Organization size, structure, and staffing
  - Process from generation to reporting
  - Source data compared to reported data
- Highlights findings and recommendations

Active Testing

- May include all parts of Passive Testing
- Injects traffic into the network or host stream.
- Compares known input with output
  - For example, inject traffic that indicates a host is compromised and sending traffic to an external host
  - Watch what you inject and any effects it may have
  - Consider creating a custom signature such as an EICAR file used in Anti-Virus testing
- Can test time to detect, notify, respond and all actions

Interfaces: Legal / Counsel

- Depending on your organization, this may be a pretty large interface:
  - Service Providers vs. Enterprise
- Tolerance of delayed / lost responses
- Process and approval flow to respond to external requests for data
  - Who does what?
  - What can be released?
  - Who must approve?

Privacy Considerations

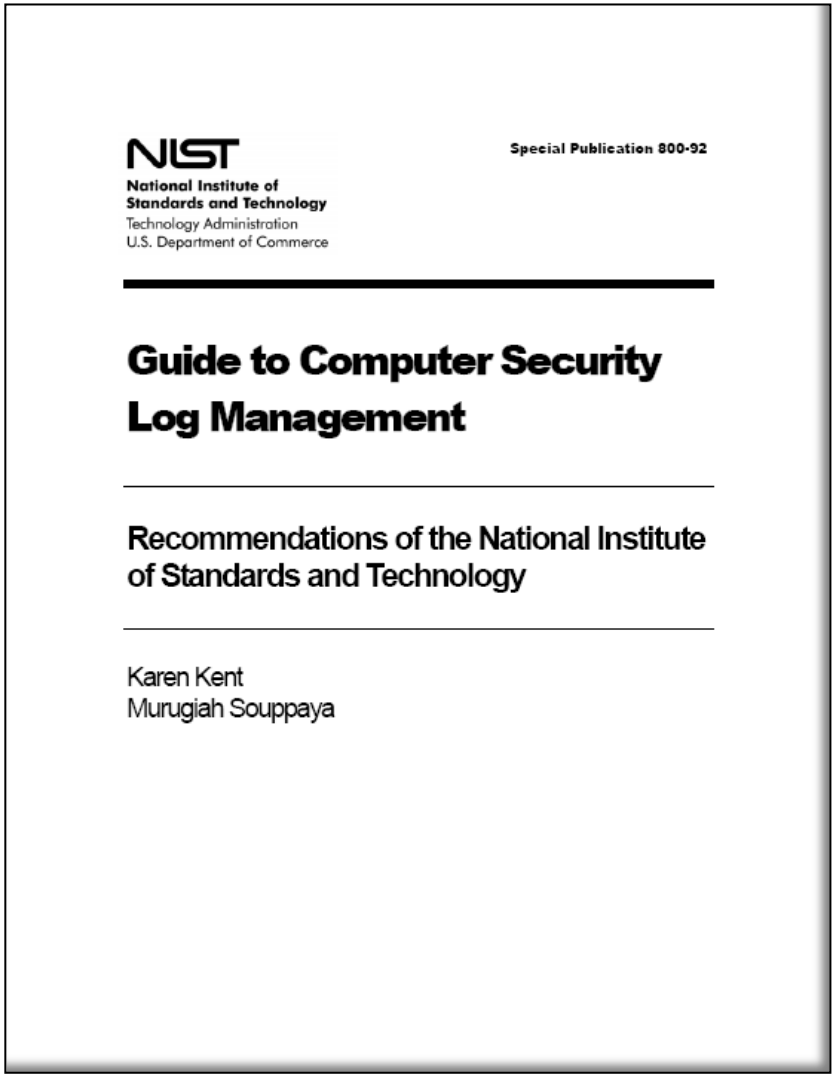
- Consider Data Protection Laws when storing and transferring information
  - Be aware of different laws where data is collected, stored, transmitted, and processed at.
- You will likely capture sensitive data
  - Both personal and corporate
- Restrict who has access to data packets
- Review logging program with Privacy and Legal teams in your organization
- Follow record retention program

Logs as Evidence: What's Different

- Must maintain Chain of Custody
- Must understand all aspects of Log Management from generation (i.e. at the node) to reporting.
  - Document the data flows. Audit it.
- Ensure file integrity. Use checksums to validate data.
- Log and review who accesses the audit logs.
- Policies and procedures must address log file preservation, chain of custody, data integrity.
- You and your logs may show up in court.

Resources:

- NIST Standard 800-92
- Vendors Product Pages and White Papers
- Compliance Standards such as HIPAA and PCI
- Computer Crimes and IP www.justice.gov/usao/eousa/foia_reading_room/usab4902.pdf



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-92

Guide to Computer Security Log Management

Recommendations of the National Institute of Standards and Technology

Karen Kent
Murugiah Souppaya

Lessons Learned

- You can't get the tuning right the first time. It's part of the process. Build the time in.
- Don't underestimate the interfaces to other parts of the organization
- Watch regulatory and industry requirements that dictate retention and on-line and off-line requirements
- In the beginning, what you log and how much you log is directly proportional to how many alerts you have
- Erring on the side of caution and alerting on more events is not always the right thing.
- Don't generate an alert if you can't won't act on it

Questions / Comments / Thoughts

- What's left?
- What's next?
- Questions? Comments? Thoughts?

Johnson & Johnson

INFORMATION TECHNOLOGY

George G. McBride

Director, IT Security Risk Management

Johnson & Johnson

1003 US Route 202, Raritan, NJ 08869 USA

T: +1.908.655.3915 M: +1.732.312.8354

gmcbri32@its.jnj.com www.jnj.com