

Data Security and Disaster Planning:

ARE YOUR RECORDS SAFE?

Presenter Bio

Michael Hintz

Assessor/I.T. Professional, Shepherd Technical Services

- 5+ years performing ISO/IEC 17025, TNI and DoD assessments
 - Accreditation Bodies: TCEQ, FL-DOH, MN-DOH, ANAB/L-A-B
 - EPA D/W Certification Officer for microbiology, organic/inorganic chemistry
- 29 years in Information Systems & Technology Field
 - Over 19 years in financial services industry
 - Extensive focus on data security & regulatory compliance
 - 20+ years designing and implementing data networks
 - 15+ years designing, implementing and testing business continuance plans
 - 10+ years performing data security audits and assessments

How Does This Apply To Me?

Think

Think

Presentation



Think



Think

Data Security and Disaster Planning Why?

Maintain Accreditation

(TNI Standard:2003 / TNI Standard:2009 / DoD QSM v5)

- Laboratory shall retain all records for a minimum of 5 years or by contractual/regulatory obligation, whichever is longer.

(includes all 'raw' data... bench sheets, logs, calibrations, original observations, etc. – not just reports)

Data Security and Disaster Planning Why?

Maintain Accreditation

(TNI Standard:2003 / TNI Standard:2009 / DoD QSM v5)

- The laboratory shall have procedures to protect and back-up records stored electronically and to prevent unauthorized access to or amendment of these records.
- In the case of records stored electronically, equivalent measures shall be taken to avoid loss or change of original data.
- All records shall be held secure and in confidence.

Data Security and Disaster Planning Why?

Maintain Accreditation

(TNI Standard:2003 / TNI Standard:2009 / DoD QSM v5)

- Records that are stored only on electronic media shall be supported by the hardware and software necessary for their retrieval.

What does that mean?!

- Think about YOUR environment...
 - Are you running MS-DOS, Windows NT, Win 95, Win 98, Win XP?
 - What version(s) of software/firmware are your instruments using?
 - What version of your LIMS system were you using 4 years ago?
Is it still supported?

Data Security and Disaster Planning Why?

- Protect the Employees (Livelihood)
- Protect the Customers (Data Custodian)
- Protect the Business (Reputation)

Data Security and Disaster Planning What?

Data (*plural noun, used with a sing. or plural verb*)

1. Numerical or other information represented in a form suitable for processing by computer.
2. Factual information, especially information organized for analysis or used to reason or make decisions.
3. Values derived from scientific experiments.

The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company.

Data Security and Disaster Planning What?

Examples of Data:

Final reports, raw analytical data, bench sheets

Traceability data (log books)

P.T. reports and supporting data

Equipment calibration & configuration records

- Model numbers, software versions

Purchasing records

Customer and vendor contact information

Data Security and Disaster Planning Where Do I Begin?

Security – Mitigating Risk

Data Security and Disaster Planning Security - Mitigating Risk

Physical Security Standards

- Controlled Access (locked rooms & file cabinets)
 - DoD QSM v5: Physical access to the servers is limited by security measures such as locating the system within a secured facility or room, and/or utilizing cipher locks or key cards.
- Records storage environment (fire, flood, humidity)
- Confidential data protection (shred policy & process)
- Record retention (archiving policy & process)
- Record destruction (purging policy & process)

Data Security and Disaster Planning Security - Mitigating Risk

Logical Security Standards

- Controlled Access (unique passwords & password policy)
 - DoD QSM v5: Individual usernames and passwords required, and must be changed at least once a year
 - DoD QSM v5: Staff trained annually in computer security awareness
- Secured network (both wired & wireless)
 - DoD QSM v5: Log-on/break-in attempts monitored; virus protection
 - DoD QSM v5: Electronic data management system is protected from the introduction of computer viruses
- Records storage environment (disks, CD's, DVD's, the 'cloud')
- Confidential data protection
 - Record storage & transmission policy & process
- Record retention (archiving policy & process)
- Record destruction (purging policy & process)

Data Security and Disaster Planning Where Do I Begin?

Disaster Planning/Business Continuance

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

➤ Start by identifying top 2 or 3 disaster 'risks'

➤ Examples:

- Fire
- Flood
- Hurricane
- Tornado
- Earthquake

Florida

1. Hurricane
2. Flood
3. Fire
4. Tornado
5. Earthquake

California

1. Earthquake
2. Fire
3. Hurricane
4. Tornado
5. Flood

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
 - Identify & involve 'subject matter experts' (SME's)
 - Delegate - each SME responsible for their area
 - Encourage 'out of the box' thinking

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
- Start Planning
 - Imagine each disaster scenario and document the steps you would take to recover
 - Brainstorm – independently AND as a group

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
- Start Planning
- Think a step (or two, or three) ahead
 - Identify and document remediation vendors
 - Identify alternative work space
 - Identify potential partnerships (reciprocal?)

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
- Start Planning
- Think a step (or two, or three) ahead
- Review and TEST the plan – then RE-test it annually
 - Can you still buy/rent the equipment you need?
 - Can you READ your backup data? (DoD QSM v5 requires it!)
 - Is vendor list still accurate? Contact information current?

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
- Start Planning
- Think a step (or two, or three) ahead
- Review and TEST the plan
- Re-evaluate your top risks

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

You can't prepare for EVERY possible risk, so...

Perform a risk assessment for YOUR laboratory

- Start by identifying top 2 or 3 disaster 'risks'
- Gather knowledge
- Start Planning
- Think a step (or two, or three) ahead
- Review and TEST the plan
- Re-evaluate your top risks
- All looks Good? Identify and plan for risk #4+

Data Security and Disaster Planning

Disaster Planning – Mitigating Risk

Food for thought...

If you showed up at your lab tomorrow and it was gone, do you have the data you need to...

- ❖ Contact your Accreditation Body?
- ❖ Contact your clients?
- ❖ Contact your vendors?
- ❖ Know where to begin the business continuance process?

Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ike



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ike



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ike



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ike



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ivan



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Physical Damage - Hurricane Ivan



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Electrical Fire Damage - Mechanical Room



Data Security and Disaster Planning

Disaster Planning - Real-World Examples

Electrical Fire Damage - Entire Lab



Data Security and Disaster Planning

Disaster Planning – Real-World Examples

Logical Damage – Virus/Malware

Large multi-location laboratory

- Corporate computer network infected by malware (computer virus)
- Negatively impacted internal network
- Remediation took WEEKS
- Significant resource impact – time AND money!

Think about this in YOUR environment...

- What if I can't access my LIMS? My instruments? My computer?
- What if I can't print reports? Send Invoices? Access client information?
- What... do... I... do... **first? Second? Third?**

Data Security and Disaster Planning

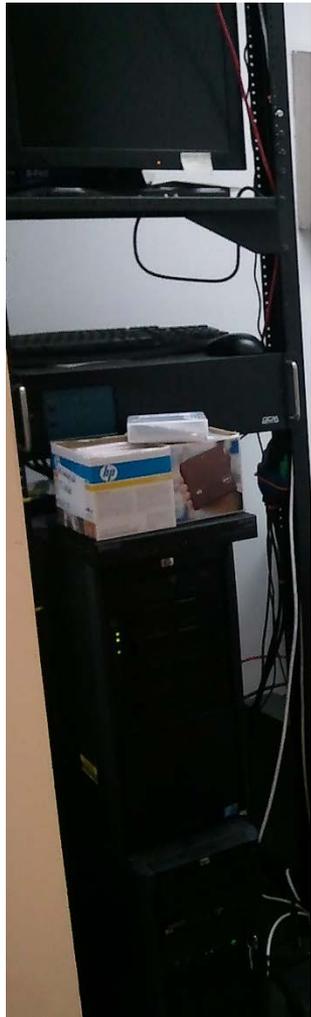
Disaster Planning - Real-World Examples

Re-Defining... Data "Dump"



Data Security and Disaster Planning

Disaster Planning - Real-World Examples



← Monitor

← Server

← Server

← Server

Re-Defining... Data "Dump"



Data Security and Disaster Planning

Disaster Planning - Real-World Examples



Re-Defining... Data "Dump"



Data Security and Disaster Planning

Disaster Planning – Real-World Examples



Re-Defining... Data “Dump”



Data Security and Disaster Planning:

ARE YOUR RECORDS SAFE?

? Questions ?

Data Security and Disaster Planning:

ARE YOUR RECORDS SAFE?

Thank you for attending!
For additional information, contact...

Michael Hintz
Shepherd Technical Services
Phone: (512) 336-1900 ext. 101
Email: MHintz@sheptechserv.com

Mike Shepherd
Shepherd Technical Services
Phone: (512) 335-0906
Email: mike@sheptechserv.com

MITIGATING RISK

Disaster Recovery/Business Continuance

Power Failure Contingency

- Uninterruptible Power Supplies on critical equipment
- Battery back-up on temperature sensors for refrigeration

Electronic vs. Paper Records & Documentation

- Electronic archiving via offsite backups and/or cloud services