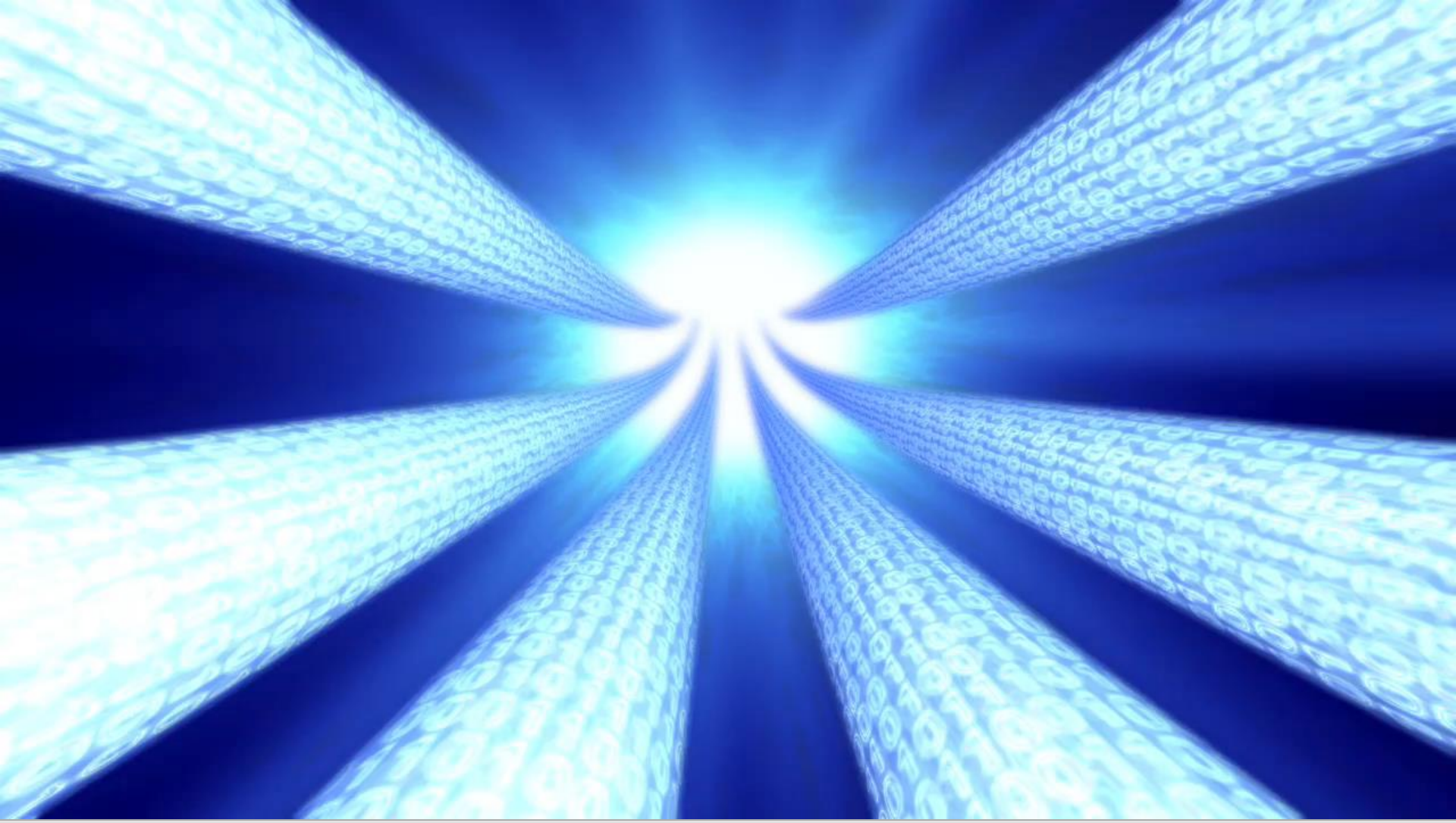


Data Loss Prevention (DLP)

Larry Yob, CISSP

Disclaimer

- The views expressed herein represent those of the presenters and do not necessarily represent the views or practices of the presenter's employer or any other party.

Agenda

- Introductions
- Progressive Protection of Data
- What is Data Loss Prevention (DLP)?
- Why is DLP necessary?
- What kind of data is at risk?
- Key Benefits/Risk Reduction
- Lessons Learned
- Big Brother
- Questions & Answers

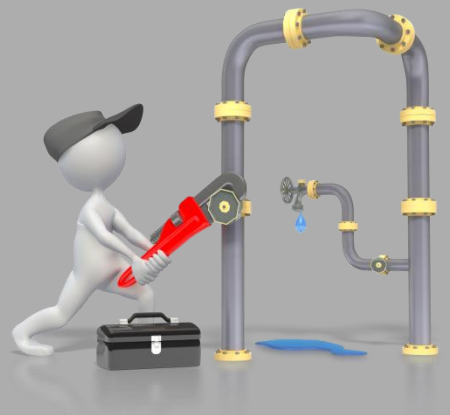
Progressive Protection of Data

- Process solutions
  - Changed recycling containers to shred bins
  - Privacy filter on computer screens
  - Secure decommission of assets and multi-function copiers had hard drives
- Technical solutions
  - Enterprise Antivirus
  - Web content filtering
  - Email encryption
  - Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
  - Desktop and laptop encryption of hard drive and USB and mass storage devices
  - Encryption of backup tapes and disks
  - Data Loss Prevention

What is DLP?

- DLP - Data Loss/Leak Prevention
  - DLP is a set of monitoring/prevention tools and processes used to identify, monitor and protect data against unauthorized transmission and possibly unauthorized use of confidential or sensitive data.

- DLP is broken down into three main system categories
  - Data in Motion
  - Data at Rest
  - Data in Use



What is DLP?

- Data in Motion – Network DLP
  - Email - corporate email
  - Web*
    - Web traffic
    - Webmail
    - Facebook
    - Twitter
    - GoogleDocs
    - File transfer protocol (FTP)
    - Instant Messaging

- Data at Rest – Storage DLP / Unstructured Data
  - Scan data on file servers, database servers, SharePoint sites, Exchange email servers

* Must have icap proxy and ssl interception

What is DLP?

- Data in Use– Endpoint DLP
  - Movement of data
  - Data written to a USB storage device and CD/DVD
  - Local printing
  - Scan data on desktop and laptop hard drives
  - Web
    - Web traffic
    - Webmail
    - Facebook
    - Twitter
    - GoogleDocs
    - File transfer protocol (FTP)
    - Instant Messaging

Why is DLP necessary?

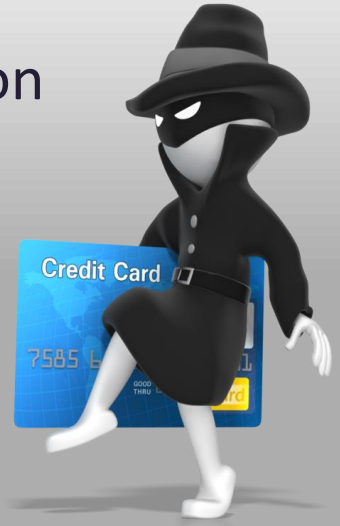
- Human error
- Accidental loss of data
- Intentional release of data
- Federal and state privacy laws
- Due diligence

What kind of data is at risk?

- Would you know if:
  - PHI was stored on a SharePoint® site, in violation of the HIPAA Security Rule?
  - A file containing thousands of names, addresses and Social Security or Credit Card numbers was sent to an external e-mail account?
  - Executive compensation records were being copied to a removable USB media device?
  - Employee copied or sent large amounts of data prior to resignation.

Types of data?

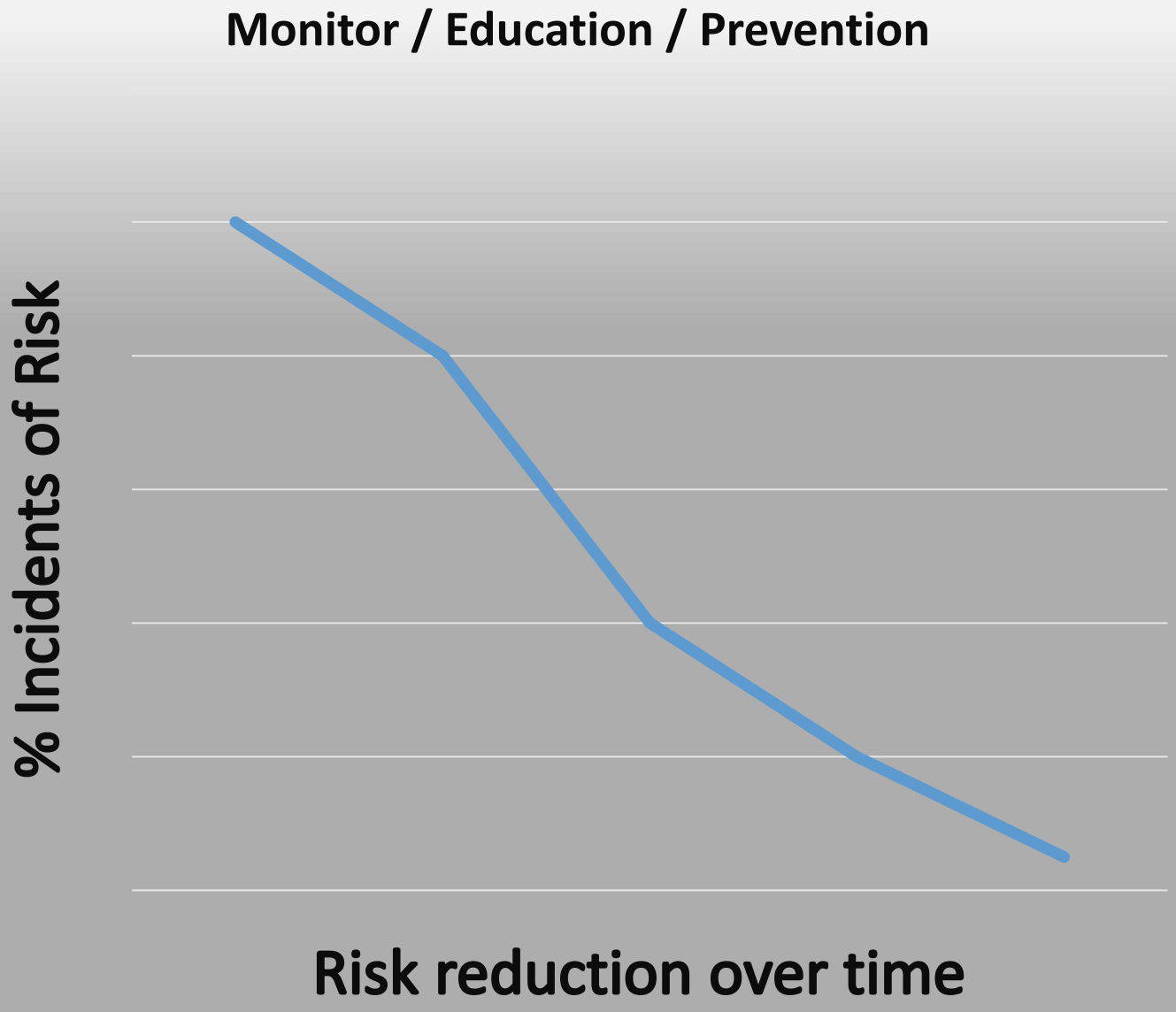
- PHI – Protected Health Information
  - Patient name, ID, diagnostic and procedure codes
  - Insurance and billing information
- PII – Personally Identifiable Information
  - Name, address, phone, SSN, DOB
- Financial
  - PCI – Payment Card Industry
  - Account information or statements
- Company Confidential
  - HR data – employee personal data, performance reviews, organization charts, layoff plans, benefits information
  - Accounting and Payroll
  - Board minutes
  - Acquisition and divestment documents
  - Contracts



Several Key Benefits

- Associate education
- Automatic restriction of sensitive data
- Monitor unauthorized access to files and documents
- Increase compliance
- Reduce incidents of data loss
  - Unauthorized transmission
  - Unauthorized use
  - Accidental disclosure

Risk Reduction



Lessons Learned

- Proof of concept (POC) - with vendor support
  - FREE
  - Virtual
  - Physical
- Pilot - with vendor support
  - FREE with some vendors
  - Start small
  - Be focused
- Keep policies at a minimum
  - Start with PCI and PII
- Professional services

Lessons Learned

- Engage all Stakeholders
  - C level executives
  - Legal
  - Human Resources
  - Corporate responsibility
  - Risk Management
- Technical teams
  - Network
  - Storage / backup
  - Server / Database / DBA
  - Security
  - Desktop / Endpoint
- International privacy rules

Lessons Learned

- FTE's - manual remediation and system support
- System reports – third party reporting tool
- Deploy in waves - no mass deployment
- Identifying challenged business processes - have solutions ready
- Communication plans
- Documentation, documentation and more documentation!

Big Brother

- DPL has the potential to scan everything. The traffic will appear to be legitimate on the network and transparent to the end user.

- Proactive controls
  - Change management
  - Reporting
  - Periodic policy and system review
  - Segregation of duties and role based access
  - Documentation, documentation, and more documentation!

Questions & Answers