SECURITY

The changing Face and Focus

UPDATED - May 2016

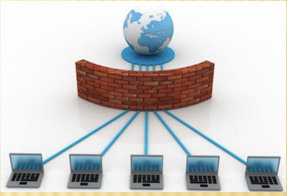
BACKGROUND

- Dick Vann
  - Sr. Advisor/Partner at PostMark
  - 21 years in corporate IT – P&G and RJ Reynolds
- PostMark
  - Mail Service Provider (MSP) in Winston Salem, NC
  - Started in 1992
  - Specializing in complex, data intensive mailing and printing

LATEST THREAT CATEGORIES

- External
- Internal – “Invited in”
- Internal – Employees
- Facilities/Physical
- Operations (Outgoing and Incoming)
- Disasters

EXTERNAL



- This is the oldest concern
- Someone outside gets in a port
- Primary protection is a firewall
- Clients seem to like to have firewall managed by an independent company
- Available as hardware with price ranges from $150 and up (significantly)
- May require subscription for updates

POSTMARK'S DECISIONS

- Split Wireless to a separate wire/IP address
- No outward facing servers (in the cloud if we need one)
- Email provided by Google (has worked very well – don't understand why email in-house)

INTERNAL – "INVITED IN" BY ACCIDENT

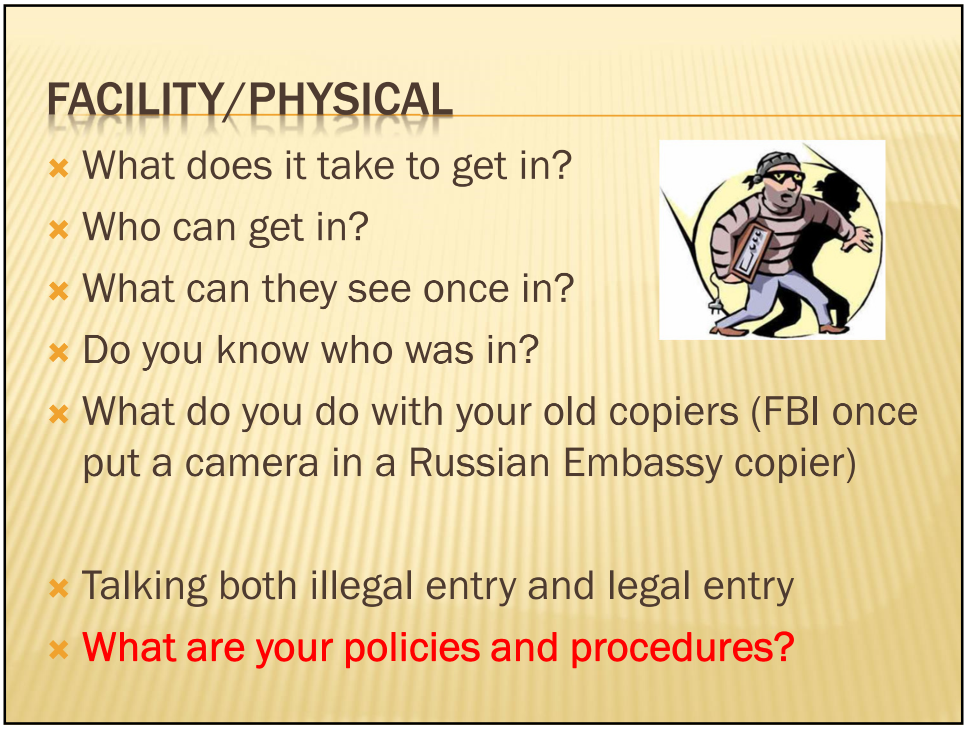
- Want a cool wallpaper for your desktop? Click here!!
- We are the IRS - read this to see why we need to talk to you.   xxxx.pdf
- Did you try using the USB drive you found in the parking lot?.
- Vendor software – how secure is their software?
- Spear-phishing – caught the Israeli power grid

INTERNAL – "INVITED IN"

- Once in – able to open door for additional software and able to id/use other vulnerabilities
- Education of employees and monitoring of employee activities is key to protection

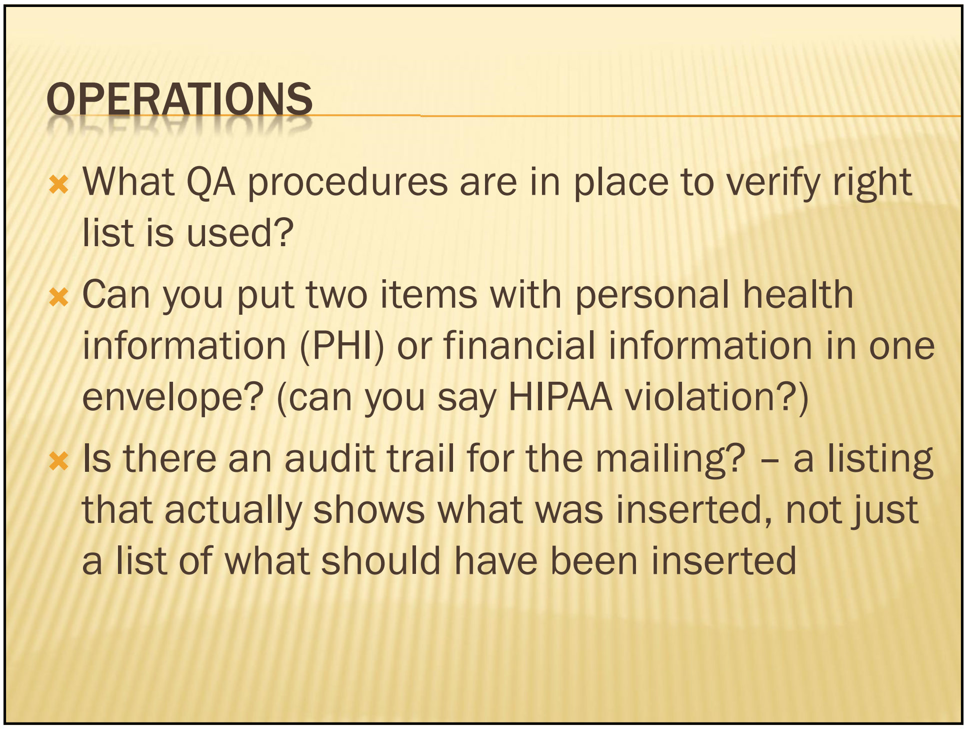
INTERNAL - EMPLOYEES

- Not all employees are happy
- Not all employees are careful
- Not all employees care
- All you need is for one to release information (Can you say Edward Snowden or Bradass87)
- New trend is to limit what employees can do and to monitor what they actually do!!
- Called Data Loss Prevention (DLP) software



FACILITY/PHYSICAL

- What does it take to get in?
- Who can get in?
- What can they see once in?
- Do you know who was in?
- What do you do with your old copiers (FBI once put a camera in a Russian Embassy copier)
- Talking both illegal entry and legal entry
- What are your policies and procedures?



OPERATIONS

- What QA procedures are in place to verify right list is used?
- Can you put two items with personal health information (PHI) or financial information in one envelope? (can you say HIPAA violation?)
- Is there an audit trail for the mailing? – a listing that actually shows what was inserted, not just a list of what should have been inserted

OPERATIONS

- How do you get/return mailing lists? FTP, email, encrypted, password, …
- Do you backup everything? – Some clients require no backup

POSTMARK'S DECISIONS

- Isolated Network
- Encrypted removable hard drives
- Encrypted USB Drives
- No email or web surfing on Isolated Network
- Data file reports to provide QA checking
- Selective backup

DISASTERS

- Fire
- Tornados
- Hurricanes
- Ice storms
- Mud slides

- Your clients want to know if their work will be done anyway!!!

DISASTER RECOVERY QUESTIONS

- What options have you formalized and TESTED?
- How easy is it to transfer the operational files and data if your plant can't operate?
- How fast do you clients expect to be operational?

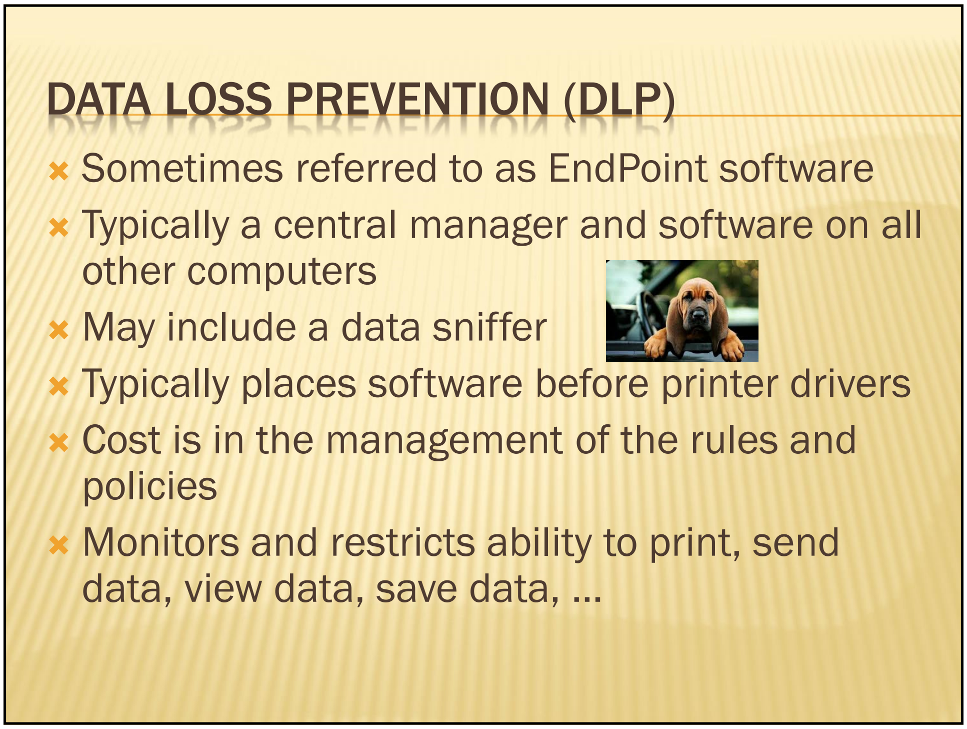
- What happens when your strategic partner asks for 50% of your capacity tomorrow?

POLICIES

- Policies must be in place to cover everything
- Training sessions must be held regularly and an attestation must be prepared
- Later audit may review implementation
- Non-disclosure agreements
- Monthly background checks
- Service personnel

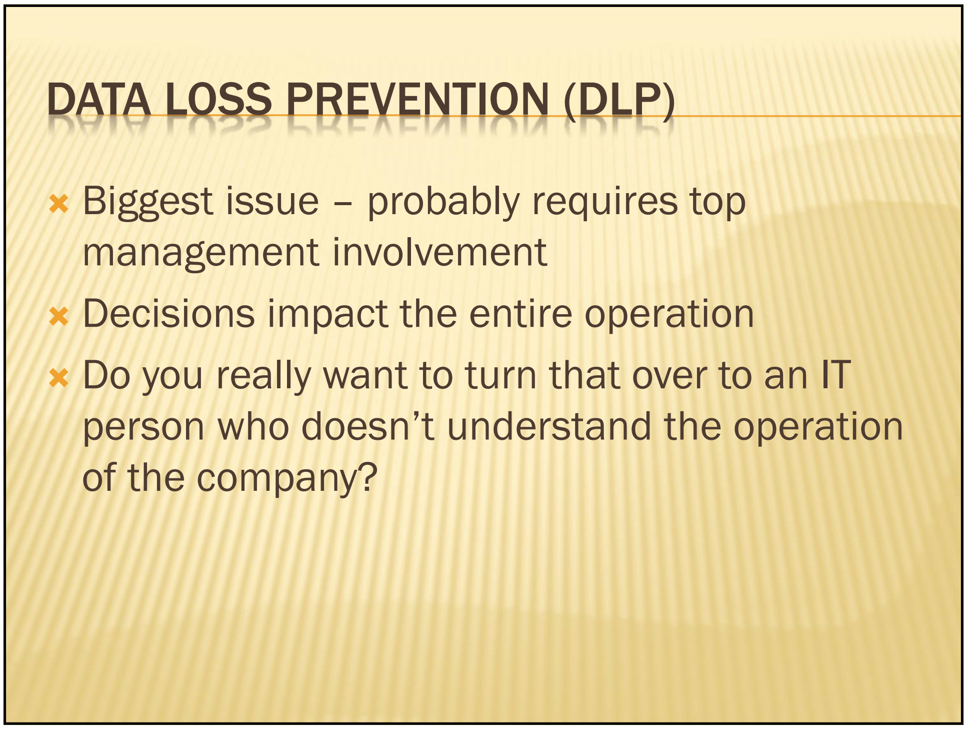
PENETRATION TESTING

- External – pretty simple
- Internal
  - OS Versions and Settings
  - Application Versions and Settings
  - User IDs and passwords
  - Equipment settings
- Initial test may run into hundreds of pages
- Fixes may range from very easy to virtually impossible – may make system inoperable



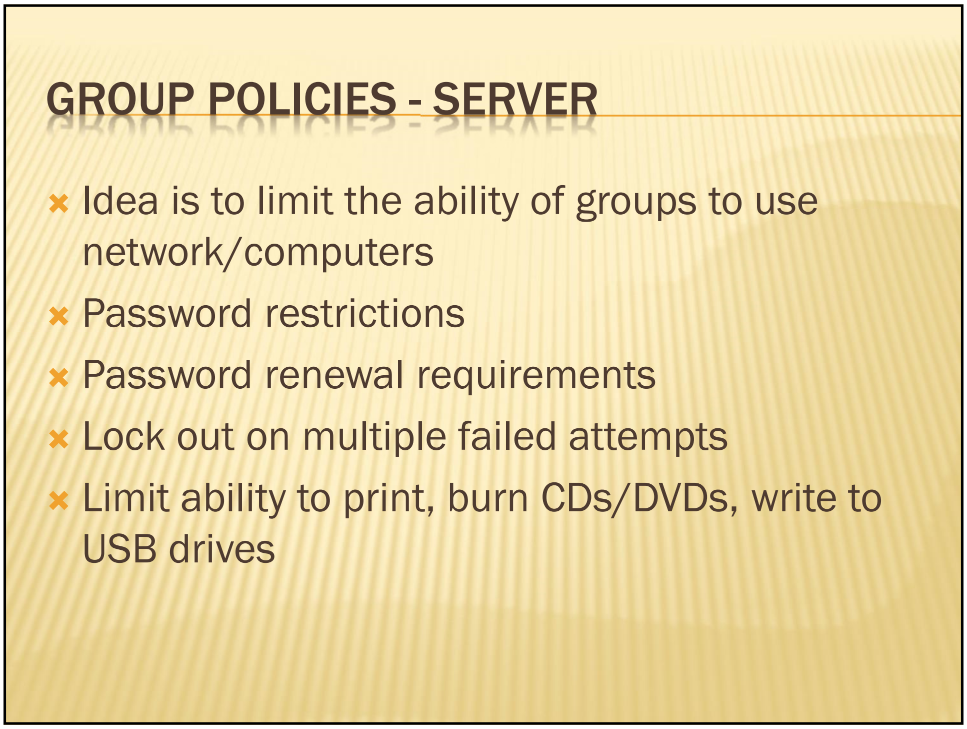
DATA LOSS PREVENTION (DLP)

- Sometimes referred to as EndPoint software
- Typically a central manager and software on all other computers
- May include a data sniffer
- Typically places software before printer drivers
- Cost is in the management of the rules and policies
- Monitors and restricts ability to print, send data, view data, save data, …



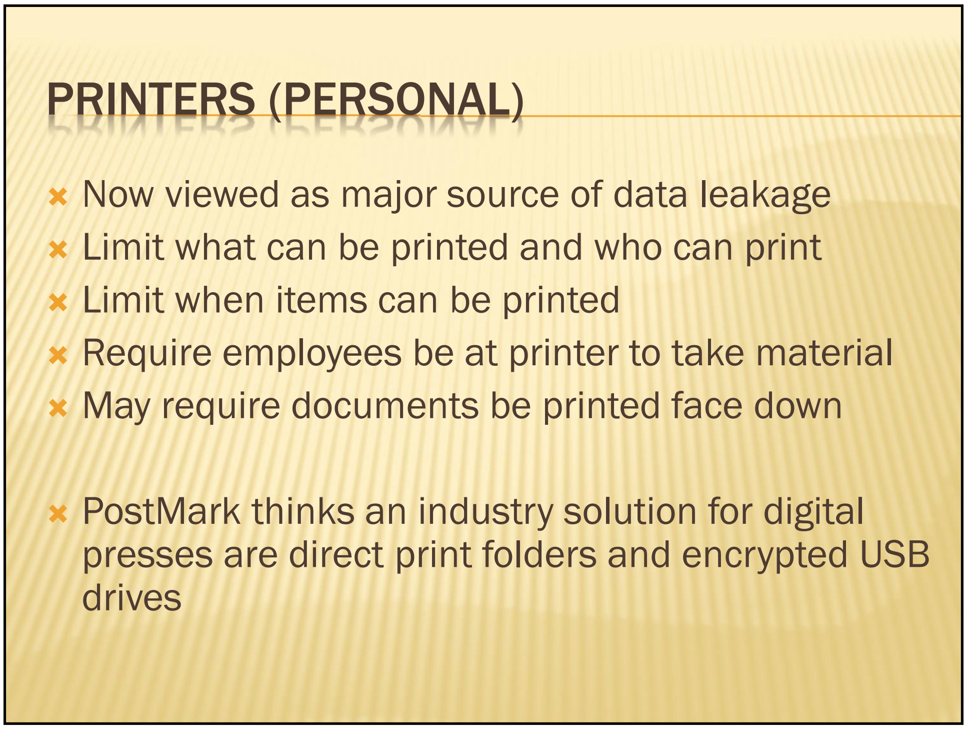
DATA LOSS PREVENTION (DLP)

- Biggest issue – probably requires top management involvement
- Decisions impact the entire operation
- Do you really want to turn that over to an IT person who doesn't understand the operation of the company?



GROUP POLICIES - SERVER

- Idea is to limit the ability of groups to use network/computers
- Password restrictions
- Password renewal requirements
- Lock out on multiple failed attempts
- Limit ability to print, burn CDs/DVDs, write to USB drives



PRINTERS (PERSONAL)

- Now viewed as major source of data leakage
- Limit what can be printed and who can print
- Limit when items can be printed
- Require employees be at printer to take material
- May require documents be printed face down

- PostMark thinks an industry solution for digital presses are direct print folders and encrypted USB drives

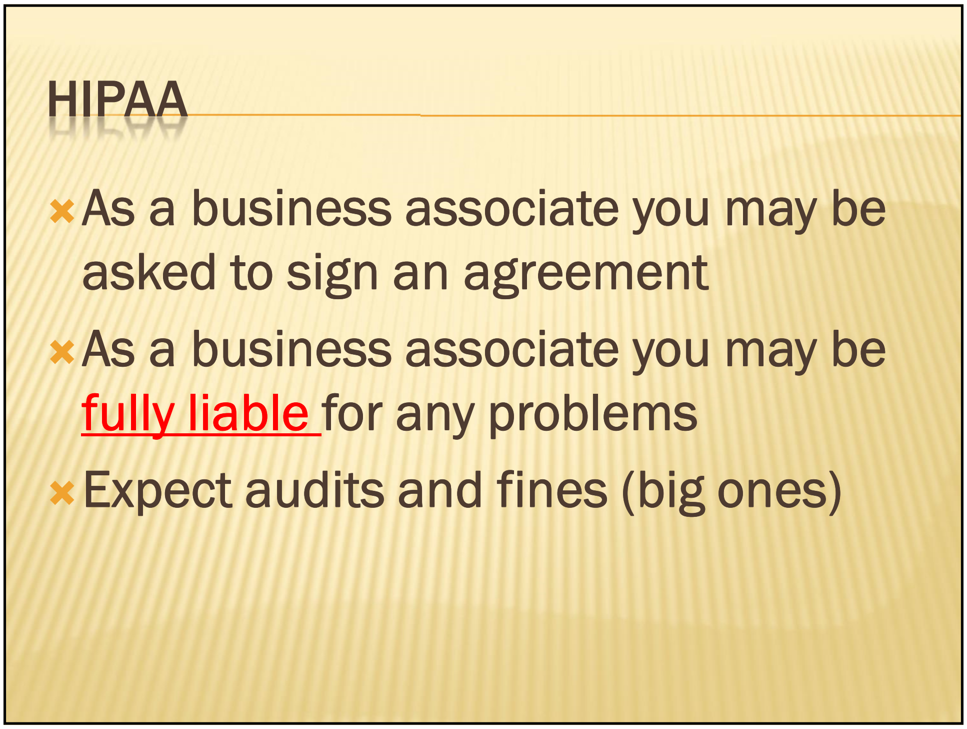
"ROGUE" DEVICES – REALLY???

- USB drives
- Tablets
- Smart phones
- WIFI (PostMark put on separate IP)
- BYOD – Bring your own devices
- Laptops must have encrypted drives

- Do you have policies in place to limit "rogue" devices?

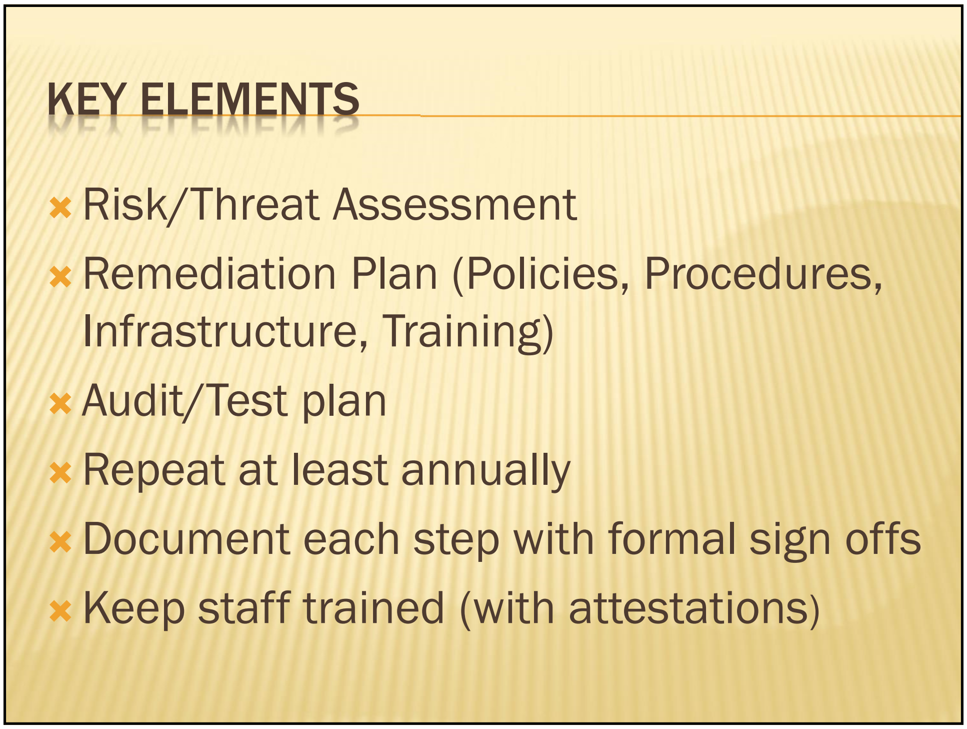
SPECIAL SECURITY CASE - HIPAA

- Health Information Portability and Accounting Act – Passed 1996
- Trick Question – Are you HIPAA Compliant?
- Answer – there is no such thing as HIPAA Compliant – it's an ongoing process



HIPAA

- As a business associate you may be asked to sign an agreement
- As a business associate you may be fully liable for any problems
- Expect audits and fines (big ones)



KEY ELEMENTS

- Risk/Threat Assessment
- Remediation Plan (Policies, Procedures, Infrastructure, Training)
- Audit/Test plan
- Repeat at least annually
- Document each step with formal sign offs
- Keep staff trained (with attestations)

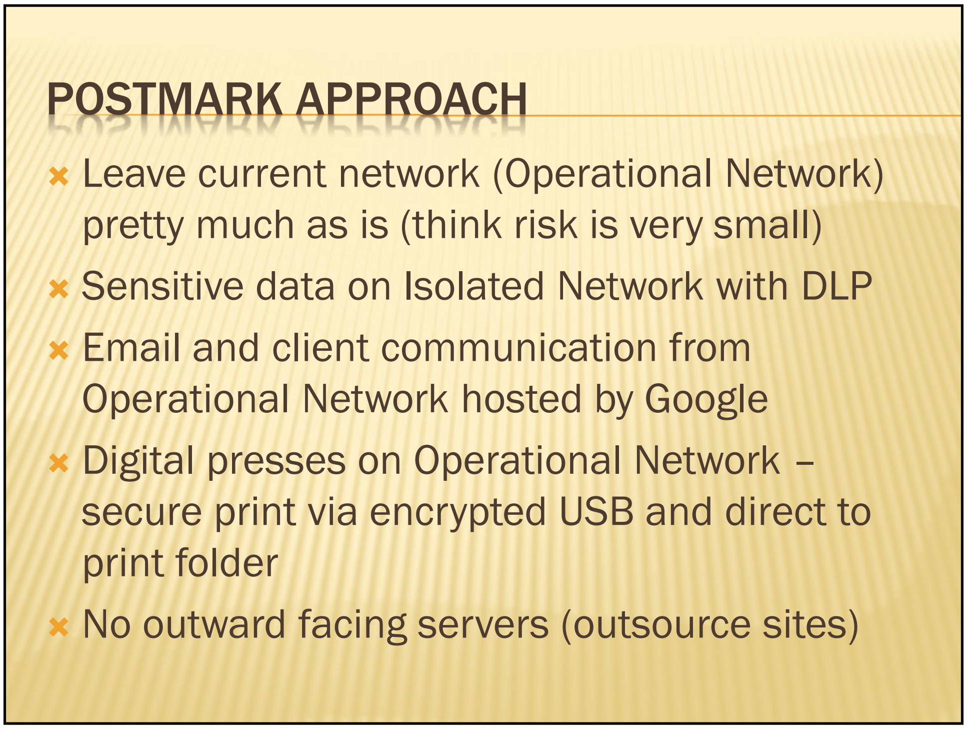
AUDITORS

- Only understand large company
- Only understand office environment
- Have to deal with very real problems
- Generally don't have responsibility to produce anything beyond a report
- Horrified to find out PostMark shares personally identifiable information (PII) with a third party

USPS – name & address on envelope

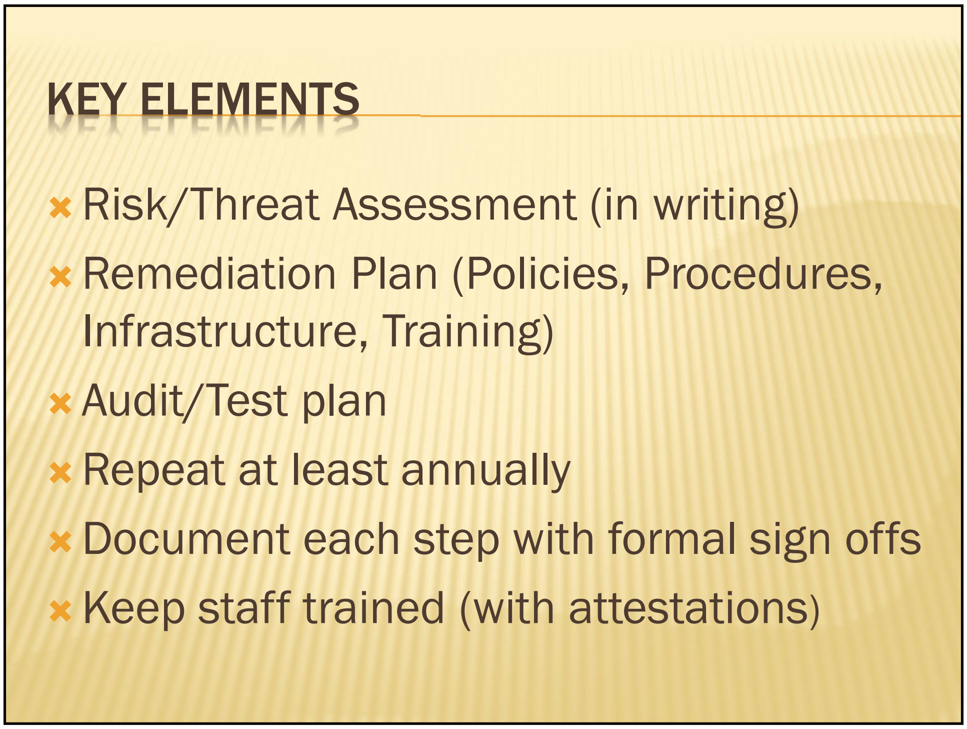
CERTIFICATIONS

- Lots of types (SSAE 16, ISO 27001, PCI DSS, COBIT, DOD, HiTrust, CyberTrust, URAC, NAIC, AUP, SOC2 Type II…) and they change
- Can be complex and expensive (but less so than a data breech)
- May be required by a client and they probably have their favorite



POSTMARK APPROACH

- Leave current network (Operational Network) pretty much as is (think risk is very small)
- Sensitive data on Isolated Network with DLP
- Email and client communication from Operational Network hosted by Google
- Digital presses on Operational Network – secure print via encrypted USB and direct to print folder
- No outward facing servers (outsource sites)



KEY ELEMENTS

- Risk/Threat Assessment (in writing)
- Remediation Plan (Policies, Procedures, Infrastructure, Training)
- Audit/Test plan
- Repeat at least annually
- Document each step with formal sign offs
- Keep staff trained (with attestations)

STAY TUNED – NEW REQUIREMENTS COMING

- 20 years ago IRS routinely printed Social Security numbers on tax form mailing labels
- 10 years ago data security was to have off site backup
- New threats are coming up every day
- The threats are **real, with dramatic consequences**

postMark

Thank you!!

Questions??????