Securing Your Documents

Heidi Alexander
Shamla Naidoo
Heidi Alexander

- Deputy Director, Lawyers Concerned for Lawyers
- Specialize in law practice management and technology
- Former practicing attorney
- Member, ABA TECHSOW Planning Board
- Author, *Evernote as a Law Practice Tool* (ABA LP Publication)

Shamla Naido

- Global Chief Information Security Officer, VP @ IBM
- Technologist for 35 years
- Lawyer for 12 years
- Law professor, building curriculum and teaching topics in information security, technology and privacy law since 2010
Agenda

- Why secure documents?
- What strategies you should adopt?
- How to do it?
- Best practices
Introduction: Why Secure Docs?

- Reminder: Lawyers Obligations
  - Competent representation and confidentiality is foundation of the attorney-client relationship.
  - ABA Model Rule 1.1 - Duty of competent representation
  - ABA Model Rule 1.6 - Duty of confidentiality
Noteworthy Incidents

• 2016: French naval contractor DCNS
  • Secret documents about its Scorpene submarines /warheads leaked.
  • The contract was worth $38 billion

• 2016: Goldman Sachs
  • Documents related to Federal Reserve Bank of New York documents leaked
  • Goldman Sachs paid $86.3 millions

• 2014: Sony Pictures Entertainment
  • Confidential contracts, employee payroll and benefit information, home addresses leaked.
  • Major reputational and financial damage
Major Causes of Breach – Internal and Inadvertent Misuse

“What were the most common ways in which the breach(es) occurred in the past 12 months?” (multiple responses accepted)

- Internal incident within our organization: 39%
- External attack targeting our organization: 27%
- External attack targeting a business partner/third-party supplier: 22%
- Internal incident within a business partner/third-party supplier’s organization: 19%
- Lost/stolen asset (e.g., smartphone, tablet, laptop, external hard drive, USB flash drive, etc.): 17%
- Both: 18%
- Abuse, malicious intent: 26%
- Inadvertent misuse, an accident: 56%

Common reasons for document leak

- Send confidential documents in clear text from the workplace using Web-based personal email accounts
- Download, temporarily store and transfer using USB drive
- Use Cloud storage (e.g. Dropbox) without permission of the employer
- Use public drive to share with coworkers
- Use public drive to collaborate with business partners

Source: Ponemon Institute survey
Why Document Security is Important? [SURVEY]

Source: Ponemon Institute survey

Figure 18. Why document-centric security is important
Two choices permitted

- Reduce the risk of insider negligence: 53%
- Reduce risks that can negatively impact the business: 50%
- Reduce the risk of malicious insiders: 31%
- Improve compliance with policies, procedures and law: 25%
- Comply with e-discovery requests: 19%
- Establish trust and confidence among users: 12%
- Enable business partners and other third parties to access information: 10%
Impacts of Document Leak

• Personal Impacts
  • Identity theft
  • Financial loss
  • Privacy

• Organizational impacts
  • Loss of customers and/or revenue
  • Loss of intellectual property or trade secrets
  • Investigative (forensic) services fees
  • Legal costs (suits, counter-suits, class-action)
  • PR communications services - damage control
  • Rebuilding brand reputation, trust, & sales pipeline

Source: https://www.shootingsportsretailer.com
http://www.indistart.com

www.techshow.com
Strategies to Secure Your Documents

- **Know Your Data**
  - Classify and label
  - Source of document generation

- **Protect** (Files, folders, USB drives, backup, archives)
  - Encryption, Watermark
  - Access control, Digital rights management

- **Monitor and Respond**
  - Access revalidation
  - Track & Revoke

- **Use Cloud with Right Controls**
  - Share the link, not the docs
  - Apply controls centrally
  - Manage and monitor

- **Education**
  - Frequent education/training

www.techshow.com
How to do it?
RUSSIA INVESTIGATION —

How Manafort’s inability to convert a PDF file to Word helped prosecutors

Former Trump campaign manager allegedly emailed doctored docs to his assistant.

TIMOTHY B. LEE - 2/23/2018, 12:15 PM
HANDS ON: Password Protection
Word Documents
Microsoft Word 2016 (Windows)
Microsoft Word 2016 (Mac)

3.4.2 Files and Folders

File and folder encryption can be a valuable tool for protecting sensitive data. It's worth understanding how to use file and folder encryption, especially if you're working with sensitive client data. If you are diligent in storing all your sensitive data in just one place. For example, say you receive an email attachment which you then open in Outlook. Ams can be stored somewhere on your desktop or downloads folder and forget about it, that is only encrypted one folder. Furthermore, if you've only encrypted one folder and you intend to access the unencrypted area of your hard drive, if you've forgotten to encrypt it, it's a simple way to protect your data.
PDF (Mac)

- Open PDF in Preview
  - Save as PDF
  - Save as PostScript...
  - Add PDF to iBooks
  - Mail PDF
  - Save PDF to Web Receipts Folder
  - Send PDF via Messages
  - Evernote
  - Edit Menu...

- PDF Security Options
  - Require password to open document
    - Password: **************
    - Verify: **************
  - Require password to copy text, images and other content
  - Require password to print document
    - Password: 
    - Verify: 

www.techshow.com

#ABATECHSHOW
Folders
Folders (Windows)
Folders (Mac)
Pitfalls of Password Protection
Bad Passwords = Easy Access

https://howsecureismypassword.net

https://haveibeenpwned.com
Lack of Control

- User retains password
- Password may be removed
- Document may be shared with others
HANDS ON: Additional Document Protection Tips
Remove Metadata
Microsoft Word (Windows)
Microsoft Word 2016 (Mac)

3.4.2 Files and Folders

File and folder encryption can be a valuable tool in securing your digital assets. If you encrypt files and folders on your hard drive, you can protect sensitive client data. If you are diligent in storing all your sensitive content, however, is that many times a problem. The problem, however, is not in the encryption itself. The problem is in the way encryption is set up.

For example, say you receive an email containing a Word document. This document is saved somewhere on your desktop or downloads folder and forget about it. The file may be downloaded to your hard drive. If you’ve encrypted the file, it’s possible that it may be accessed in an unencrypted area of your hard drive. This can potentially result in a security breach.

Word for Mac allows you to encrypt files and folders. From the menu, go to Security > Security. Create a password to secure the document. You can also encrypt PDFs with Mac’s native Preview tool. To use this feature, go to File > Security > Encryption. Then, go to File > Disk Utility and select the folder you wish to encrypt. After you have created the encrypted disk image, delete the original folder.
Adobe Acrobat DC

- Tools:
  - Redact: Permanently delete sensitive text, graphics, or hidden data
  - Remove Hidden Information
  - Sanitize Document

- Enhance Scans:
- Create PDF
- Edit PDF
- Export PDF
- Comment
- Organize Pages
- Protect
- Fill & Sign
- Prepare Form
Full Disk Encryption
Windows Bitlocker

![Windows Bitlocker Control Panel](image)
Mac FileVault

FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk “Macintosh HD”.

Click the lock to prevent further changes.
Best Practices for You

• What you should do?

✓ Classify the document appropriately based on the sensitivity
✓ Apply appropriate security protections
   ✓ Encrypt, Access controls, digital rights management
   ✓ Encrypt the files/folders where appropriate
✓ Apply care when forwarding or distributing sensitive documents, avoid sending the documents instead consider sharing link to where document can be accessed
✓ Use only approved document repositories in the organization
Best Practices for Your Organization

• What should your organization do?
  ✓ Deploy technologies to classify, protect, and monitor documents
  ✓ Consider digital rights management
  ✓ Prevent documents from being accidentally or maliciously forwarded
  ✓ Removing access to documents at any time even from an unsecured PC or mobile device
  ✓ Use cloud based solutions to collaborate (share the links but don’t send the actual documents)
  ✓ Enabling users to send files and collaborate with business partners or other outside parties
  ✓ Educate employees
Thank You & Questions

Heidi Alexander
Heidi@masslomap.org

Shamla Naidoo
ibmciso@us.ibm.com
• YOU play the most important part in keeping TECHSHOW exciting. *Please complete the Speaker evaluation before you leave.*

• Reserve the dates!

TECHSHOW 2019: February 27 – March 2, 2019