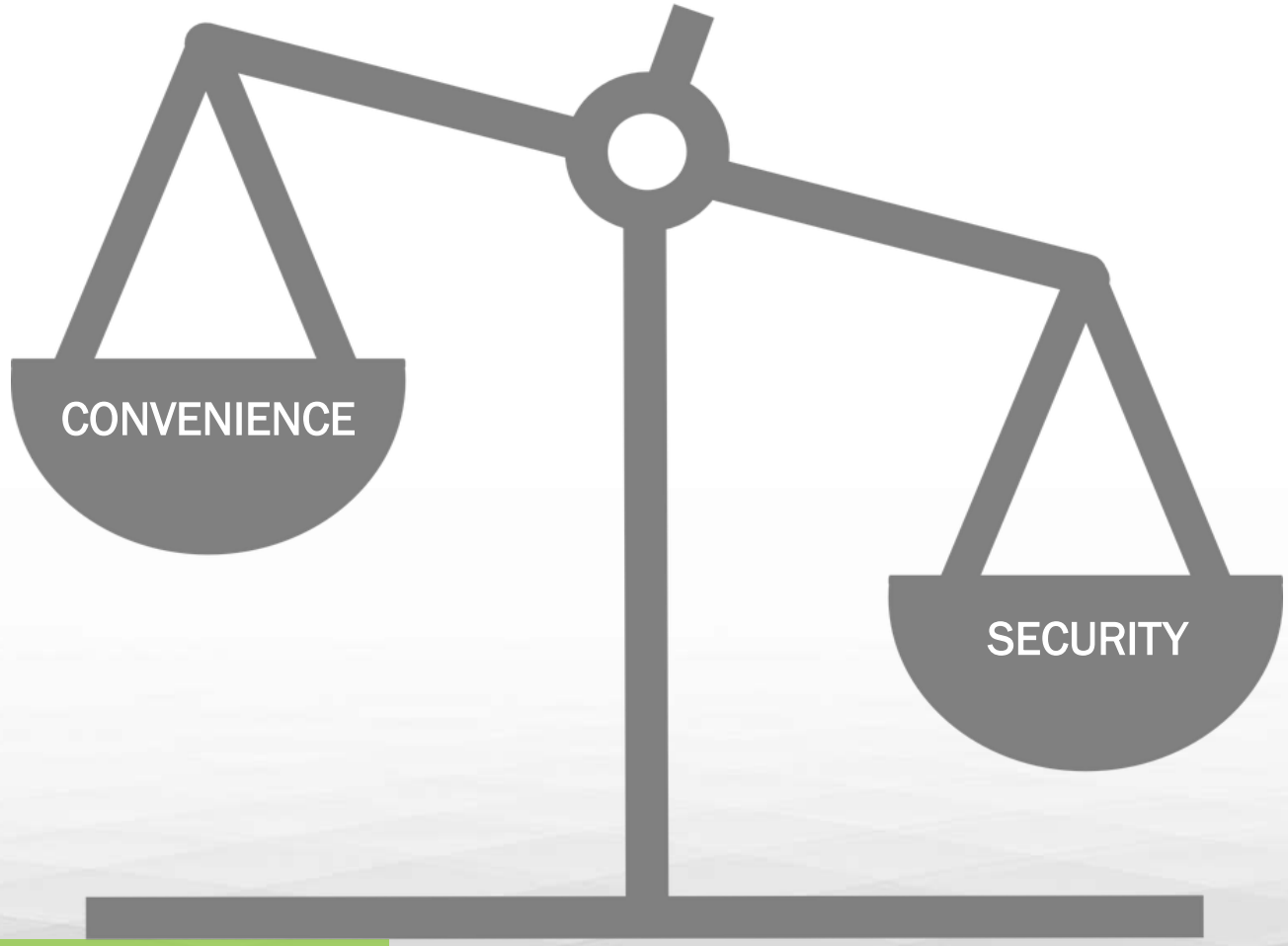
Worldox

www.worldox.com

Cyber Security Education and Planning

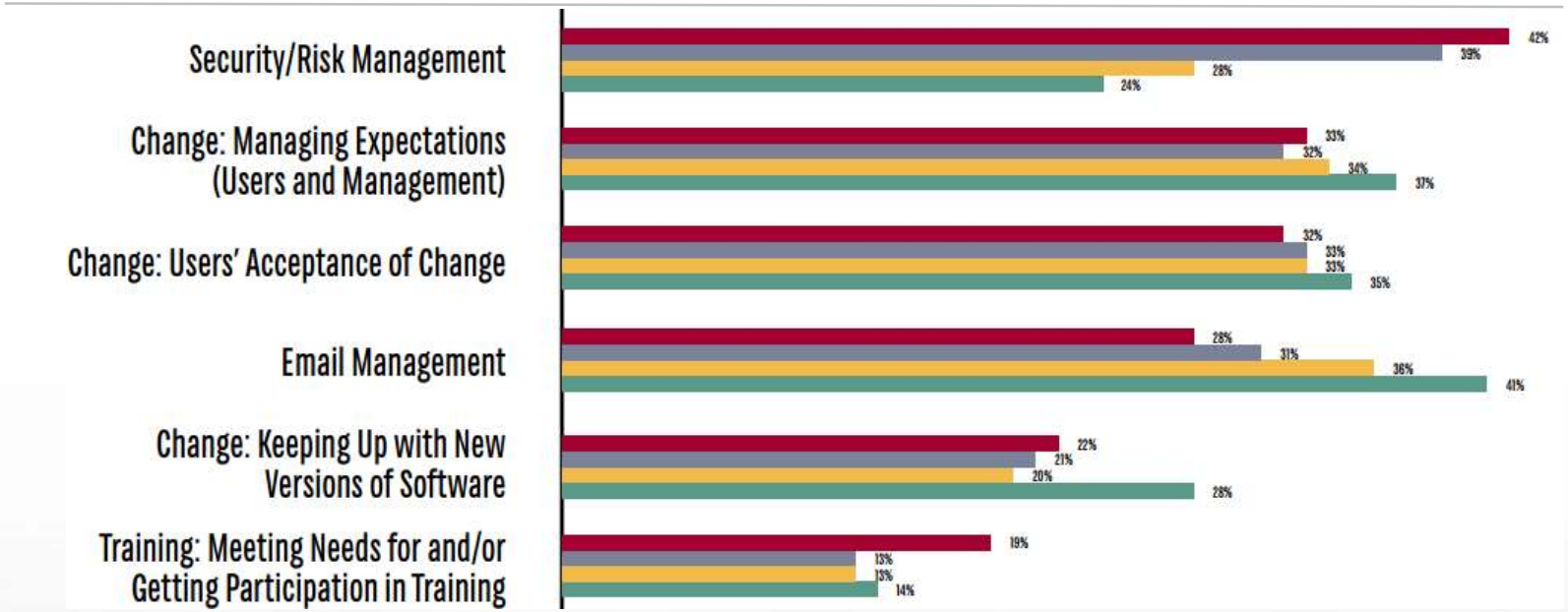
Why isn’t everyone prioritizing Security?



Security Top Concern

ILTA Technology Survey 2015

What are the top 3 issues or annoyances within your firm?



Trending data 2015-2012

Learning the Hard Way

In the news…

MOSSACK FONSECA

In April 2016, 11.5 million files and 2.6 terabytes were hacked from the database of the world's fourth biggest offshore law firm, Mossack Fonseca. The incident is known as the Panama Papers.

The documents show, among other things, how clients – including high profile politicians – allegedly hid assets.

TARGET
110 million individual's contact information stolen

Neiman Marcus
350,000 individual's credit card information stolen

Michaels
2.6 million individual's credit card information stolen

YAHOO!
Email service for 1 billion users hacked

aaronbrothers ART & FRAMING
400,000 credit and debit cards were compromised

at&t
Hacked from within for two weeks

ebay
Cyber attack led to access of 223 million user accounts

feedly
15 million users affected by denial-of-service attacks

EVERNOTE
100 million users affected by denial-of-service attacks

P.F. CHANG'S CHINA BISTRO
Credit card information for 33 locations was stolen and sold

CHS Community Health Systems, Inc.
Personal data for 4.5 million patients compromised

SUPERVALU
Personal data from multiple locations compromised

ups
Customer data from 60 store locations stolen including financial data

The Home Depot
56 million shopper's credit card information stolen

Google
5 million Gmail username and passwords stolen

iCloud
Online data storage hacked to post celebrities' private photos online

goodwill
880,000 customer's credit card information stolen from 330 stores

FBI Warnings to Law Firms

FBI Alert Warns of Criminals Seeking Access to Law Firm Networks

March 11, 2016

COMMENTARY

5/31/2016
09:06 AM

Panama Papers Fallout: What If Your Lawyer Gets Hacked?

MARKETS

Hackers Breach Law Firms, Including Cravath and Weil Gotshal

Investigators explore whether cybercriminals wanted information for insider trading

Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert

Learning the Hard Way

In the news…

BUSINESS | LAW

Global Law Firm DLA Piper Faces Disruptions After Cyberattack

'Petya' ransomware attack limits access to firm's computer systems, email

By *Jacob Gershman* and *Kate Fazzini*
June 29, 2017 3:16 p.m. ET

Bloomberg Businessweek

Thank You for Calling Equifax. Your Business Is Not Important to Us

Credit monitoring in the U.S. is a nightmare. It only took a massive public data breach to make that clear.

ABA model rules

Rule 1.1 – Competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology,*** engage in continuing study and education and comply with all continuing Legal education requirements to which the lawyer is subject.

Rule 1.6 – Confidentiality of Information

…(c) ***if the lawyer has made reasonable efforts to prevent the access or disclosure.*** Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Formal Opinion 477R

…In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

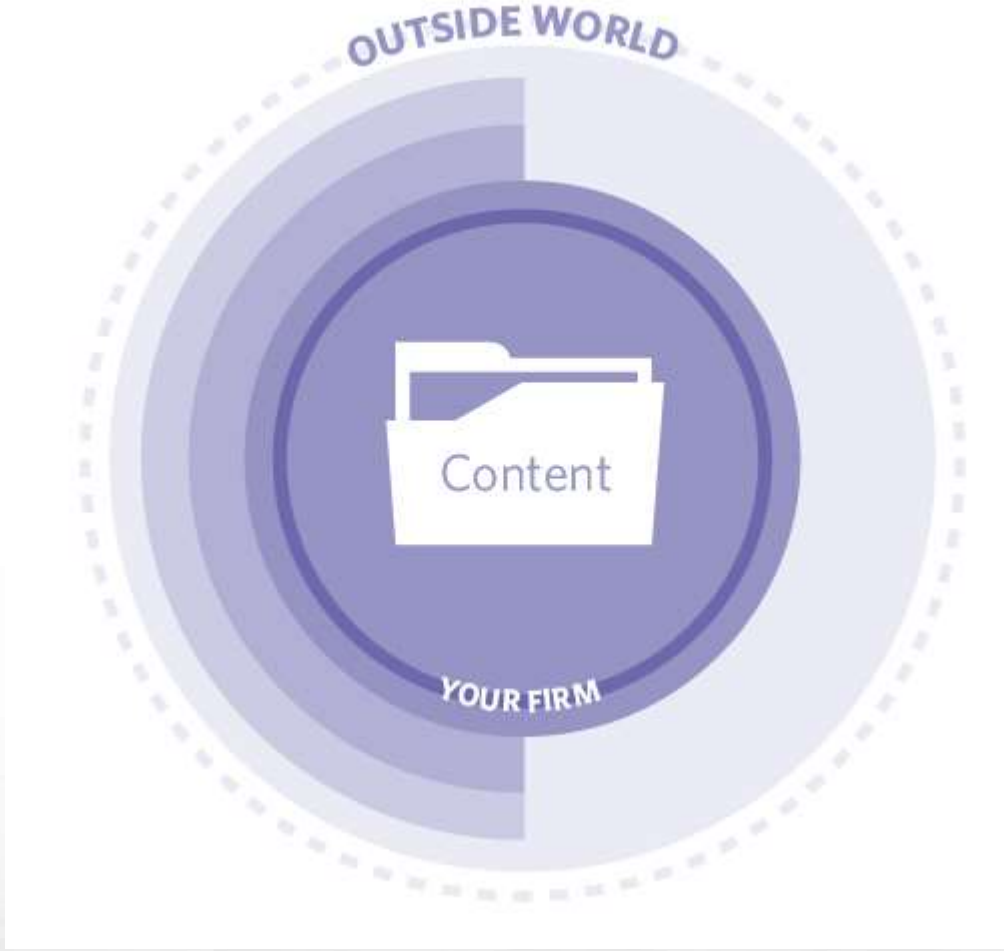
However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable - Formal Opinion 477R at p. 5

Reality

III. SECURITY PROGRAM—FRAMEWORKS AND STANDARDS

- http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat
- Mandiant Intelligence Center Report, APT1: Exposing One of China's Cyber Espionage Units, page 20, available at http://www.mandiant.com.
- Westby, Jody R., "Cybersecurity and Law Firms: A Business Risk," Law Practice Magazine, Vol. 39, No. 4, available at http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-lawfirms.html
- International Organization of Standardization (ISO), the 27000 series11, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- Information Technology Infrastructure Library (ITIL), http://itil-officialsite.com
- International Society of Automation (ISA), http://www.isa.org
- ISACA, COBIT, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- Payment Card Industry Security Standards Council (PCI SSC), https://www.pcisecuritystandards.org/security_standards/documents.php
- National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS), http://csrc.nist.gov
- Information Security Forum (ISF) Standard of Good Practice for Information Security, https://www.securityforum.org/?page=publicdownload2011sogp
- Carnegie Mellon University Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), http://cert.org/octave
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP), nerc.com/page.php?cid=2|20
- U.S. Nuclear Regulatory Commission, nrc-stp.ornl.gov/slo/regguide571.pdf
- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capabilitymaturity-model-es-c2m2

20,000 ft view



Security Layers

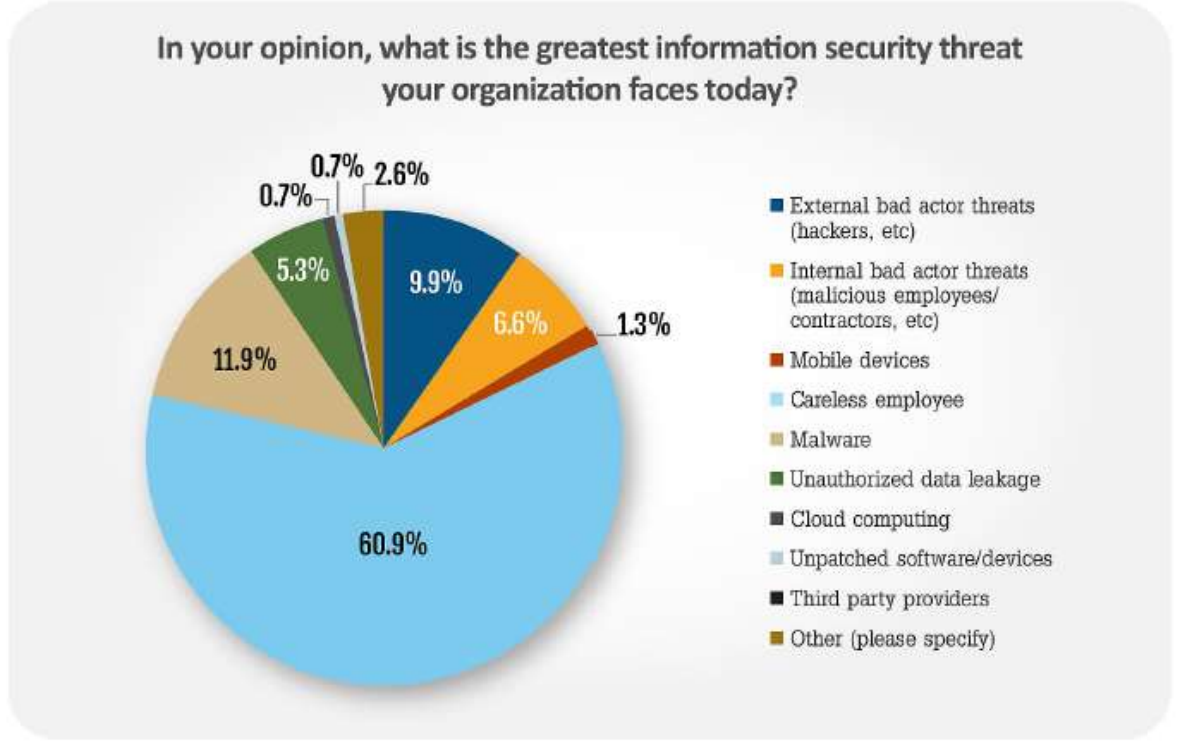
Current	Planned	Proactive
• Network Perimeter / Firewall • AD • Locks • Access logs • Alarms • Authentication	• Education • Password / Dual Factor Authentication • File Sharing • Remote Access • Secure Collaboration	• Risk Assessment • Proactive Penetration Testing • Archive/Delete • Pessimistic Model • Encryption • Education • DRM • MDM/MAM • Intrusion Detection

Who's the bad guy?

Hackers?

Employees with bad practices

- Lack education and training
- Choose weak passwords
- Share login credentials
- Install applications without consulting IT
- Upload company files to personal cloud storage
- Access company data after changing jobs
- Not careful enough with Email



250 Hackers Surveyed

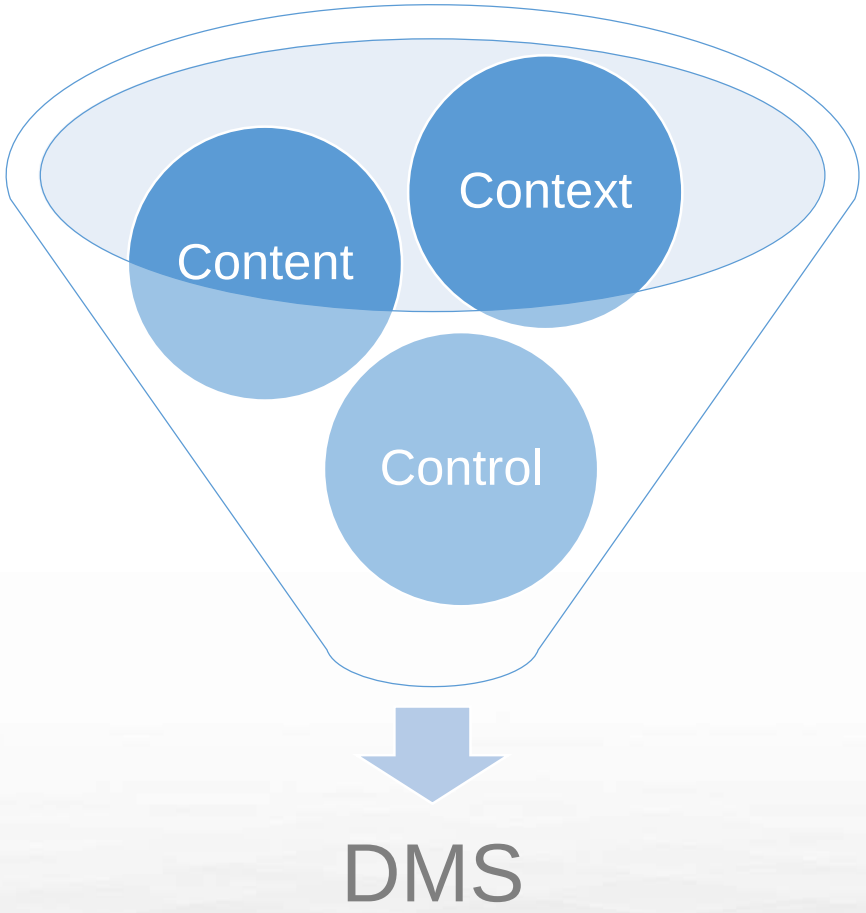
- “Remembering and changing passwords” noted by hackers as top source of cyber fatigue.
- Multi-factor authentication and encryption are the biggest hacker obstacles.
- 31% cited access to privileged accounts as best entry point with access to an email account a close second at 27%.

Black Hat 2017: Hacker Survey Report

More than four out of five blame humans for security breaches

With perimeter security technologies considered largely irrelevant, hackers are focusing more on gaining access to privileged accounts and email passwords by exploiting human vulnerabilities. Indeed, more than 85% of Black Hat survey participants named humans as most responsible for security breaches. Unpatched software (10%) and insufficient security technology (5%) were far behind.

Risk Assessment



Know Your Data (Information Governance)

Recognize what confidential / private data you maintain

- Social Security Numbers
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Intellectual Property
- M & A deals

Where does it reside in space and time?

Is it organized in such a way that it can be easily secured?

Law firms are not exempt from litigation holds

Where is your data?

On premises or in the Cloud?

Mobile Devices?

Laptops?

File Sharing products?

How is your data organized?

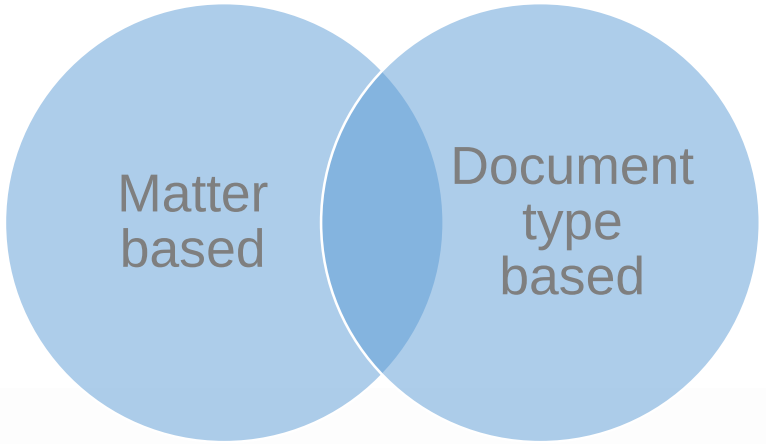
Does your firm have standards by which documents are saved and organized?

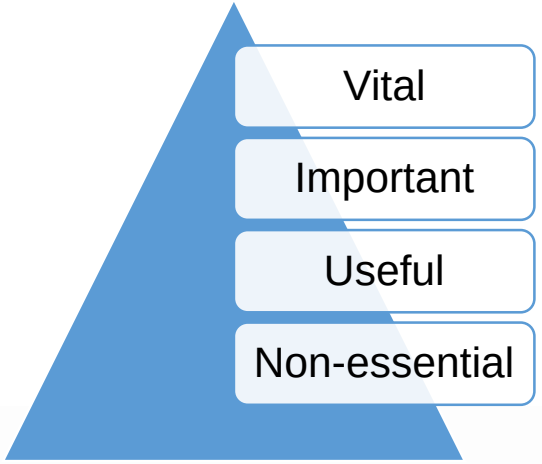
Do you have a Document Management System (DMS)?

Is your data organized by client and matter?

Document Retention

- Accounting & Finance
- Corporate and Exemption
- Correspondence / Internal Memoranda
- Email
- Employment, Personnel Records
- Case Information





Software Updates

- Windows / Office Updates
  (https://technet.microsoft.com/en-us/security)
- Antivirus Software
- Enhanced Mitigation Experience Toolkit (EMET) (EOL: July 31, 2018)
- Firewall
- Virtual Private Network (VPN)

Preventing Data Loss

- Examine applications for leakage potential
- Risk assessment on each to determine potential exposure
- Application analysis for leakage potential
- Procedural analysis for leakage potential
- Ongoing risk assessment
- Shadow IT

Training, Policies & Procedures

- **User Education and Cooperation**: without buy in from the top, security awareness education will not be taken seriously.
- **Policies**: ensure employees understand the rules and why they are important; security awareness will benefit them at work *and* at home.
- **Procedures**: ensure employees know how to use systems properly and securely.

Password Policies

https://hitachi-id.com/password-manager/docs/password-management-best-practices.pdf

Password Policies

Forget Tough Passwords: New Guidelines Make It Simple

August 14, 2017 · 4:51 PM ET
Heard on All Things Considered

"The traditional guidance is actually producing passwords that are easy for bad guys and hard for legitimate users," says Paul Grassi, senior standards and technology adviser at NIST, who led the new revision of guidelines.

The organization suggests keeping passwords simple, long and memorable. Phrases, lowercase letters and typical English words work well, Grassi tells NPR's Audie Cornish. Experts no longer suggest special characters and a mix of lower and uppercase letters. And passwords never need to expire.

COMPUTER SECURITY

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

NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

http://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple

Dual Factor Authentication

https://duo.com

Free for up to 10 users

$3 / user / month

Phishing

Example Phishing attempt

From: Amazon.com [mailto:amazon@amazon-sales.com]
Sent: Monday, February 13, 2017 10:18 AM
To: Ray Zwiefelhofer <ray@worldox.com>
Subject: Your Amazon.com order has shipped (#658-52786270-3542243023)

amazon

Shipping Confirmation

Hello,

Your order "Apple iPhone 7 AT&T 128 GB (Jet Black) Locked to AT&T" has shipped.

Below you can find the invoice and the shipping details.

Details

Order #658-52786270-3542243023

Expected delivery date:
February 13, 2017

Total including shipping:
$669.99

Order details

Depending on the ship speed you chose, it may take 24 hours for tracking information to be available in your account.

We hope to see you again soon.

Amazon.com Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the sellers business

Phishing Mitigation

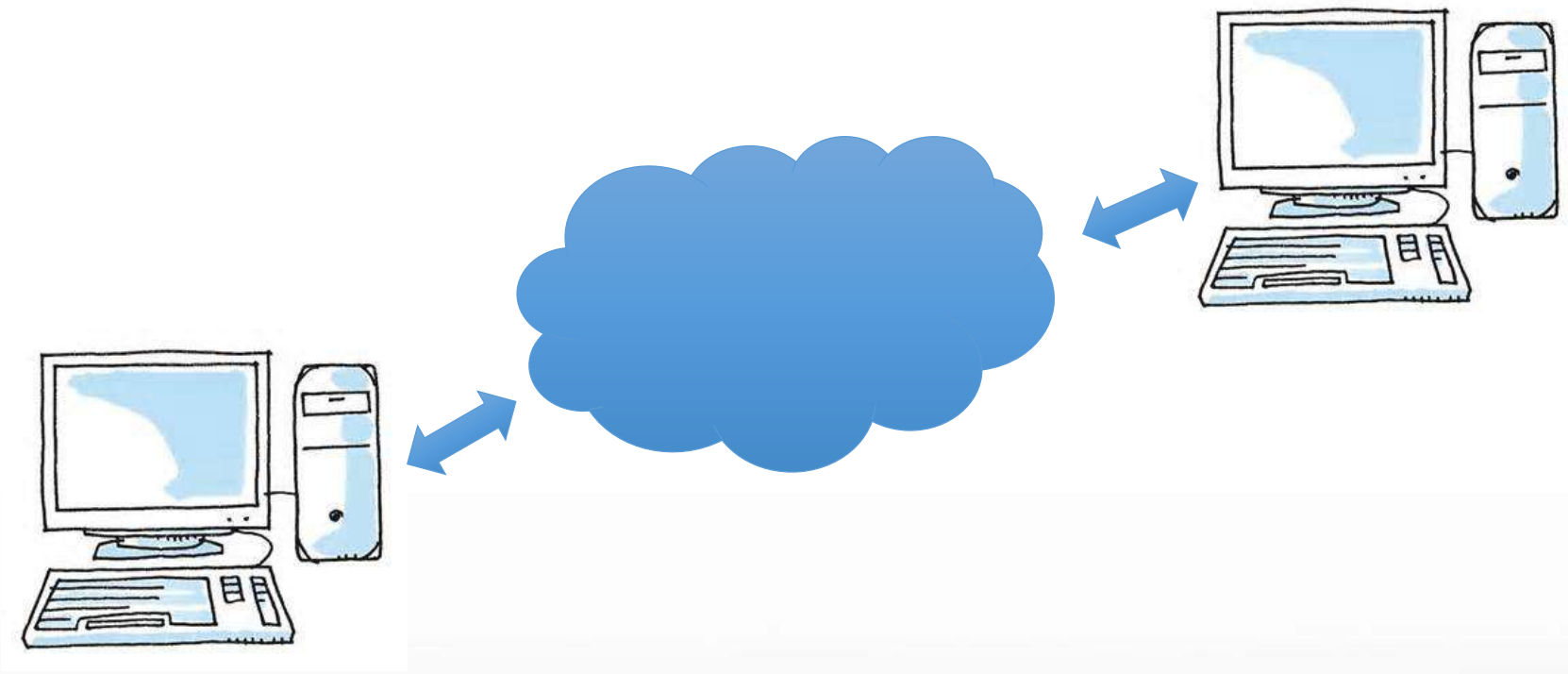
1. Eliminate access to Personal Email accounts on work computers.

2. Sandbox incoming attachments
    1. Mimecast
    2. Office 365 Advanced Threat Protection

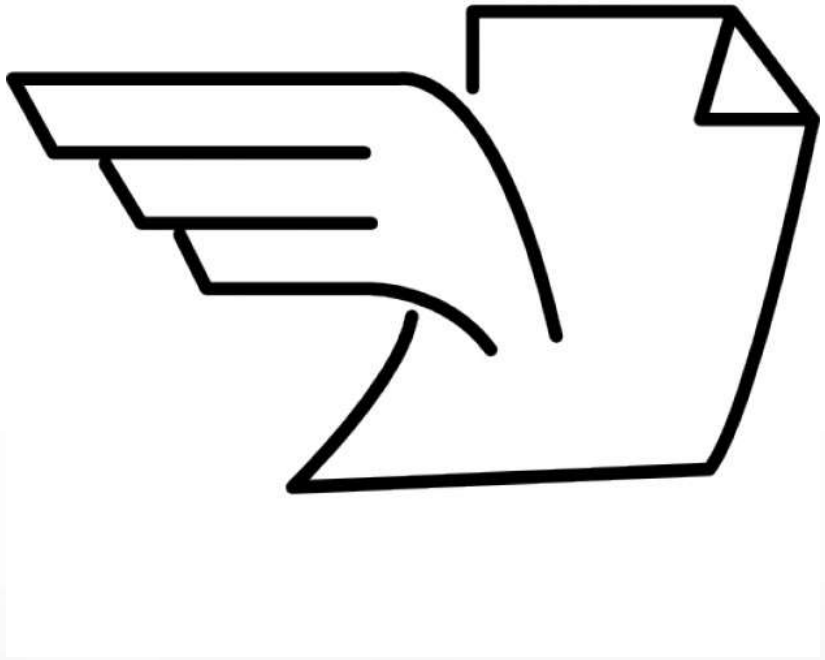
Least Privilege

Unique User Accounts

Remote Content Access



Sharing and Collaboration



Bring Your Own Device (BYOD)

Intrusion Detection Services

$4000 + monthly

Dedicated Devices and 24/7 Staffing

http://www.guardsite.com/Intrusion-Prevention-Service.asp

Penetration Testing

Type	Description	Starting Price, USD
External Network	Price is for an external penetration test addressing security vulnerabilities at the network layer* and also including host configuration** vulnerabilities, up to 32 IP addresses.	$3,000
Internal Network	Price is for an internal penetration test (on your internal network) addressing security vulnerabilities at the network layer* and also including host configuration** vulnerabilities, up to 32 IP addresses.	$4,000
Web Application	Price is for a single web application penetration test, in conjunction with an external or internal network penetration test.	$1,200
Wireless	Price is for a wireless penetration test, in conjunction with an internal network penetration test, for one wireless access point and associated client devices.	$3,000
Social Engineering	Price is for a Remote social engineering test, including two separate electronic attack vectors including spear phishing email directed at human targets within your organization, in conjunction with an external network penetration test***.	$3,000

http://highbitsecurity.com

Encryption

How a DMS can help

Information Governance

Retention Policies

Active Directory Integration

Ethical Walls

Audit Trail

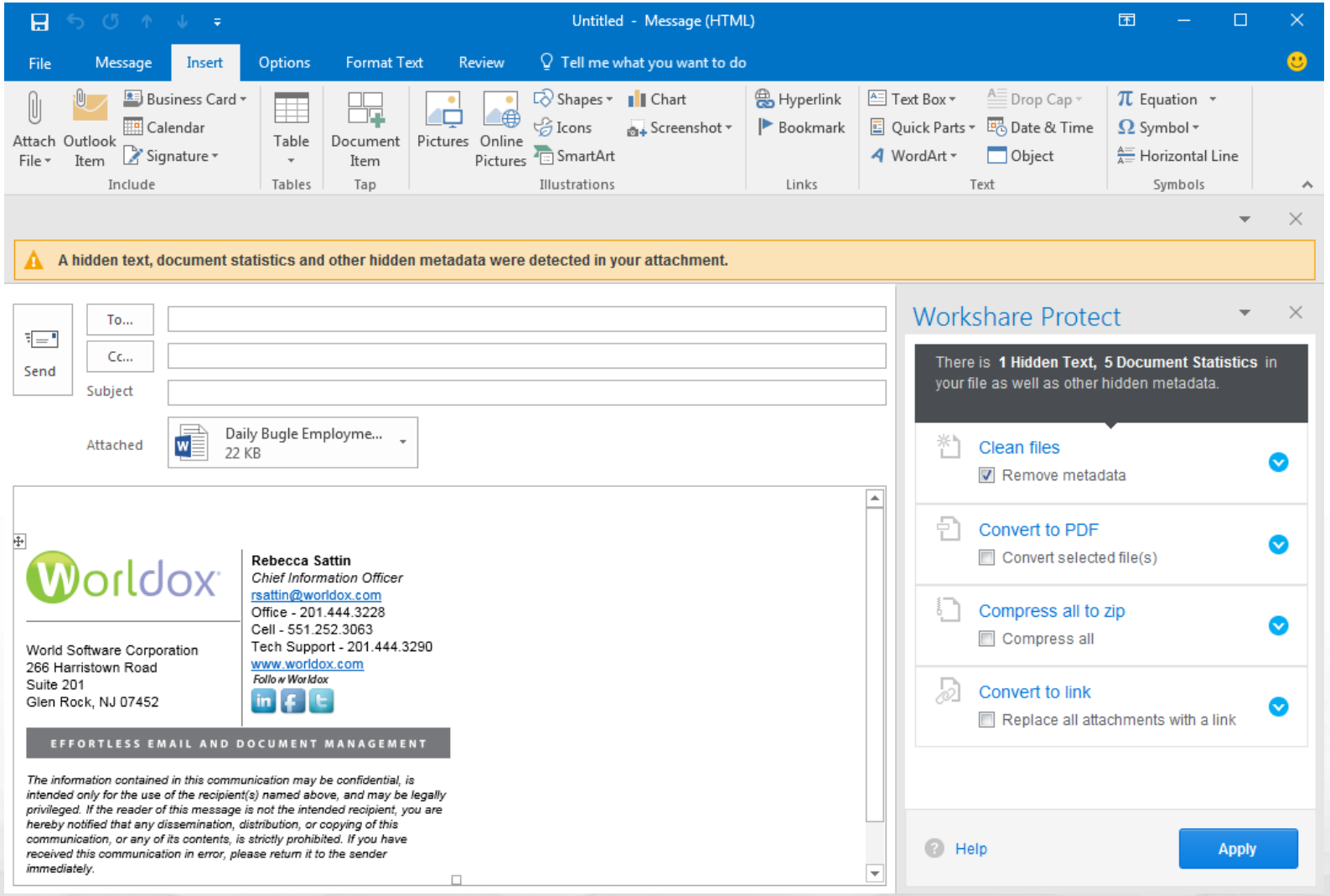
Encryption

What World Software is doing

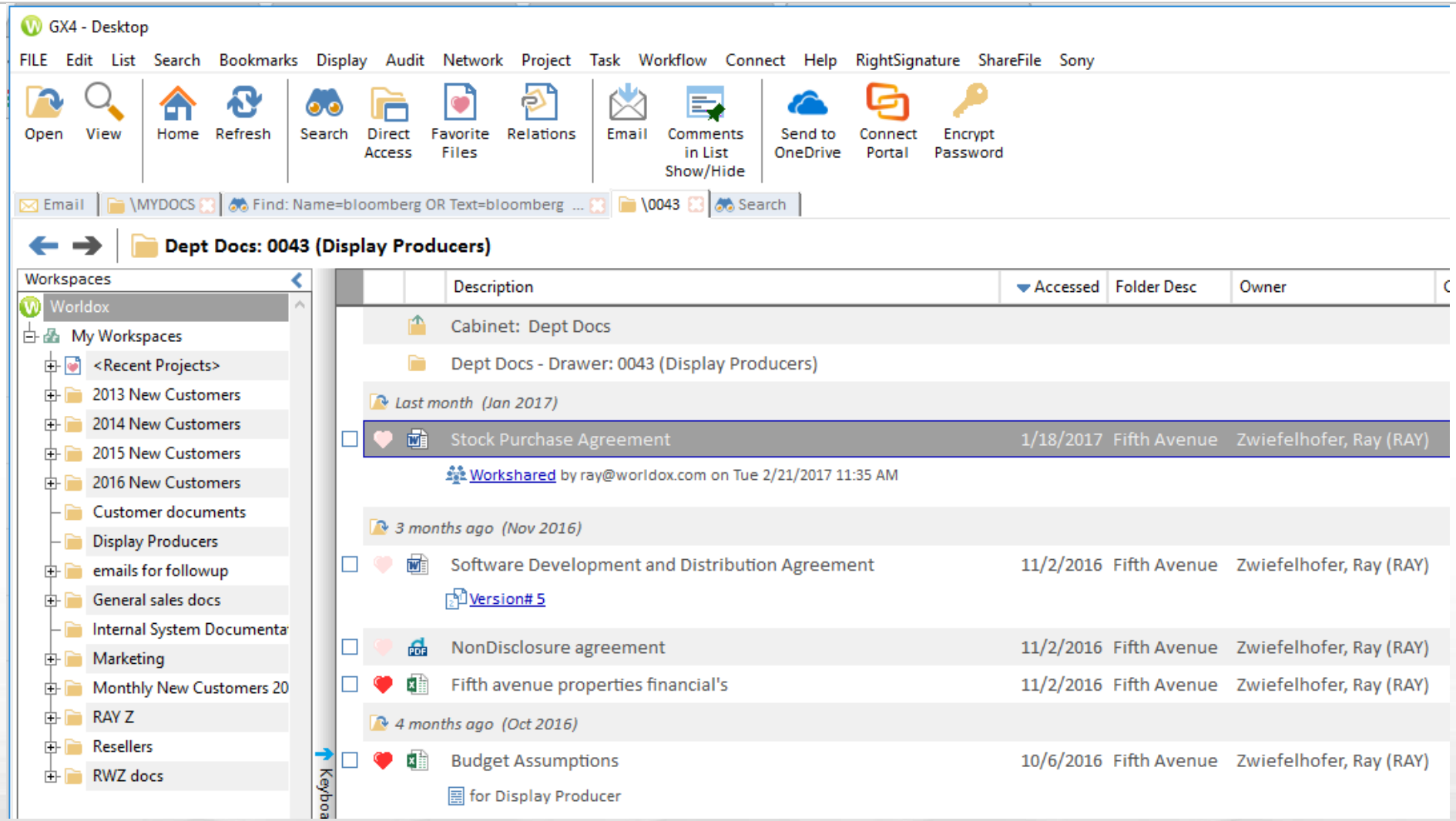
- Worldox Encryption At Rest (WEAR)
  includes delegated Cabinet control with secondary certificate
- Worldox Connect
  sharing with accountability

Secure Content Framework

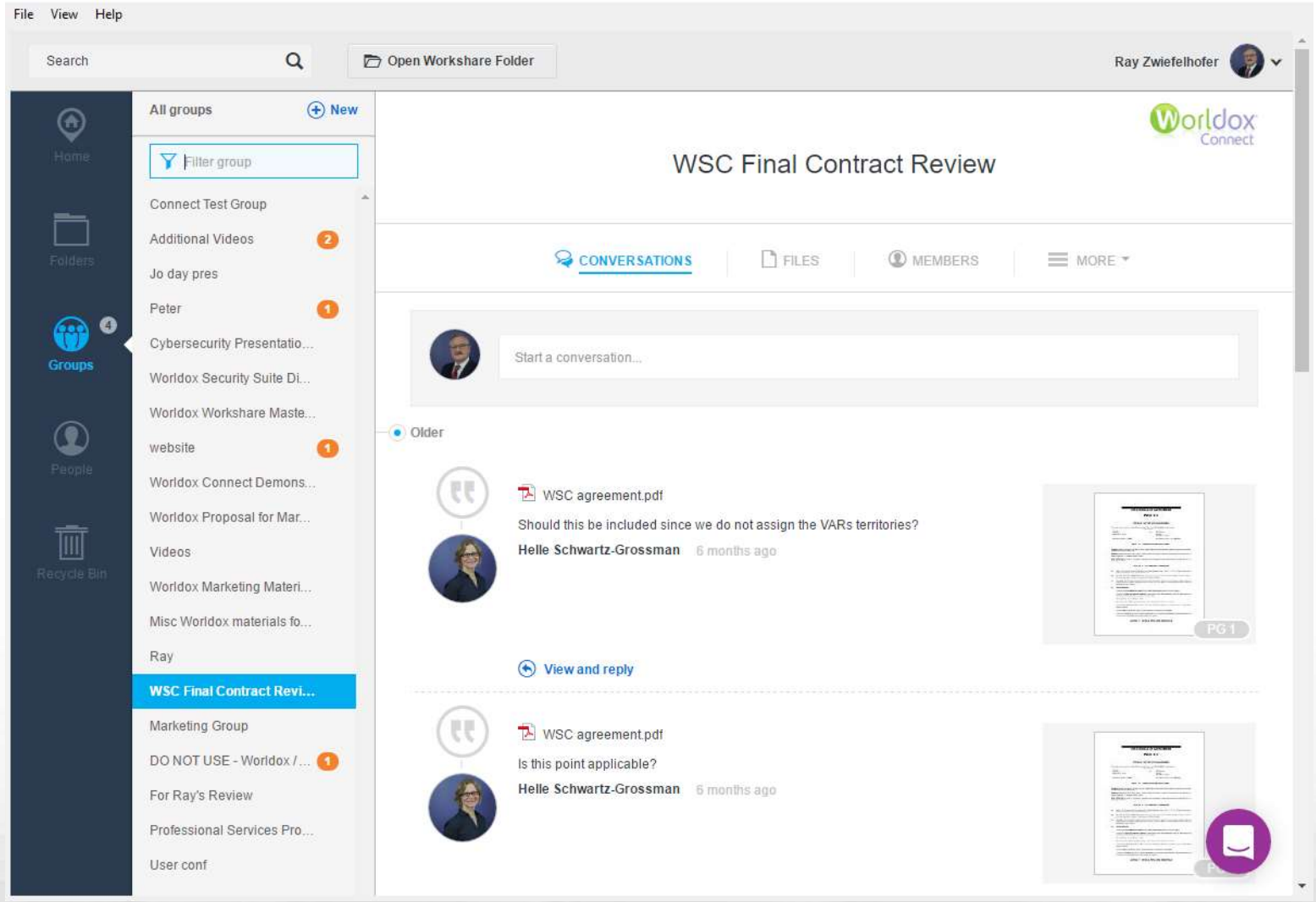
Secure Sharing



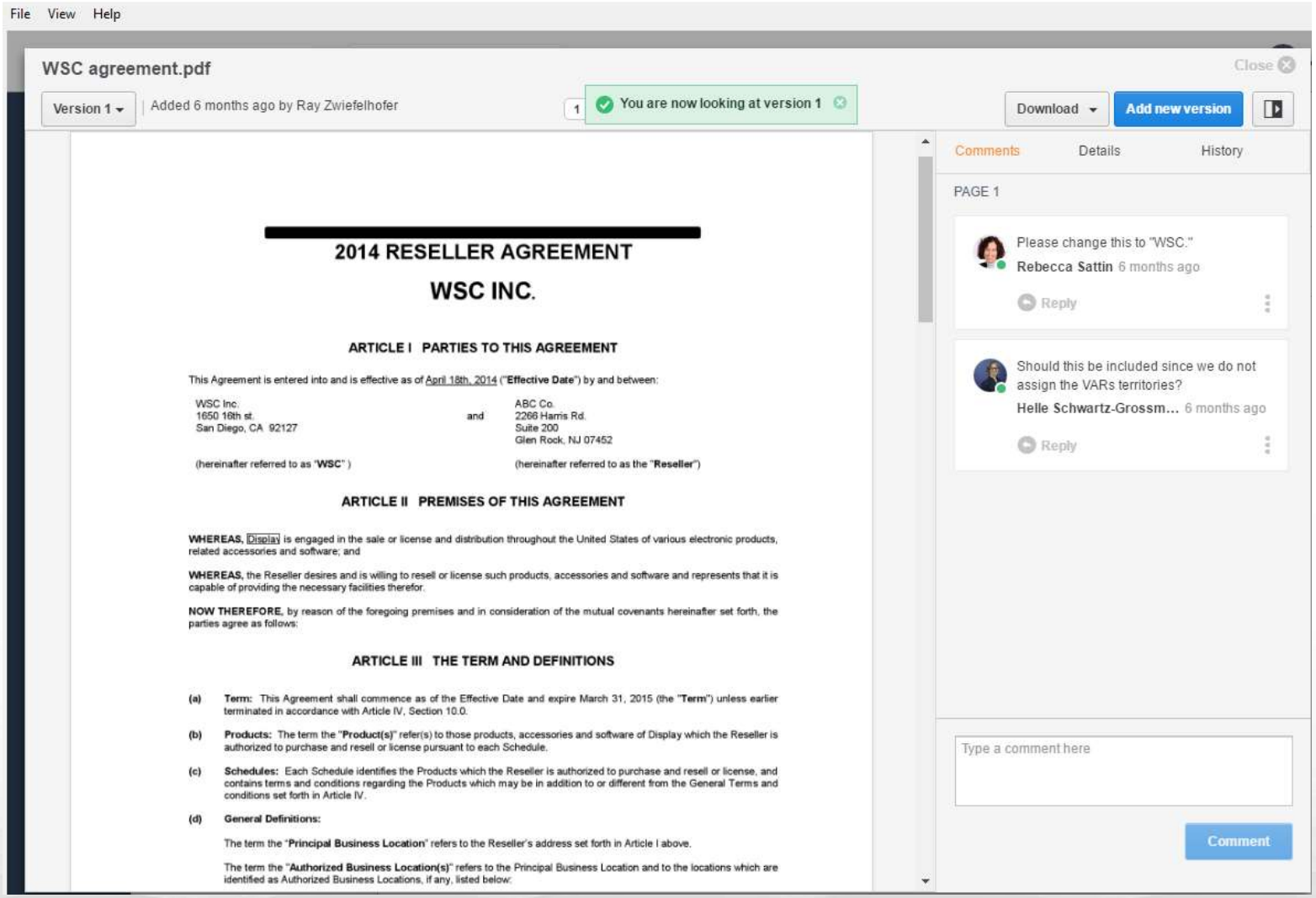
Worldox Integrated Sharing



Secure Collaboration



Secure Collaboration



Mobile Content Management

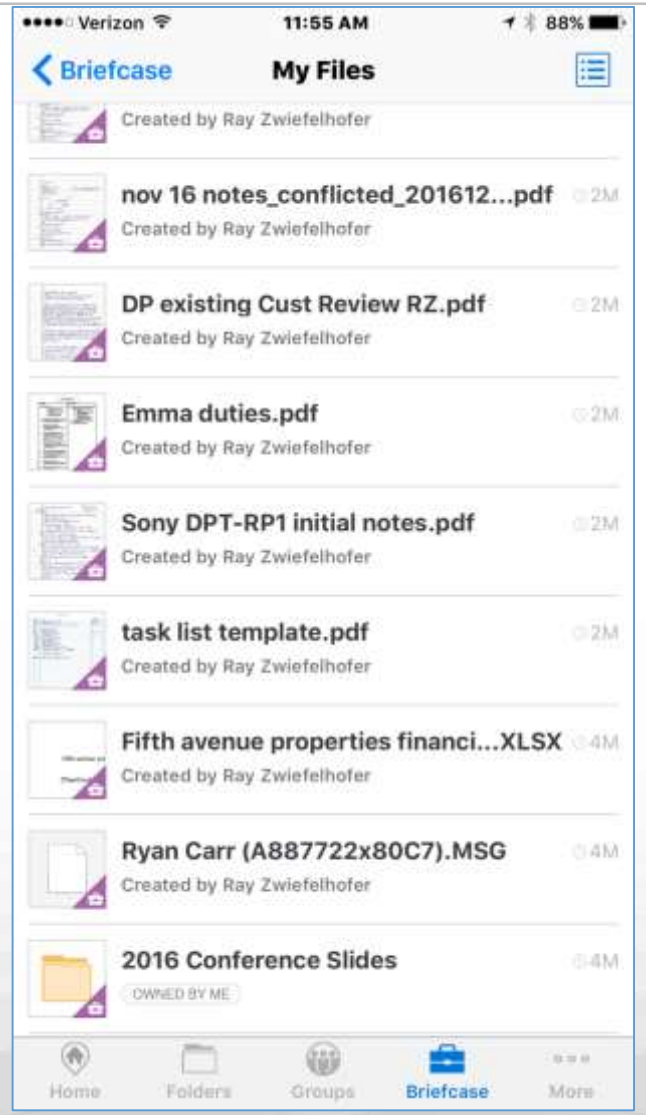
All Devices

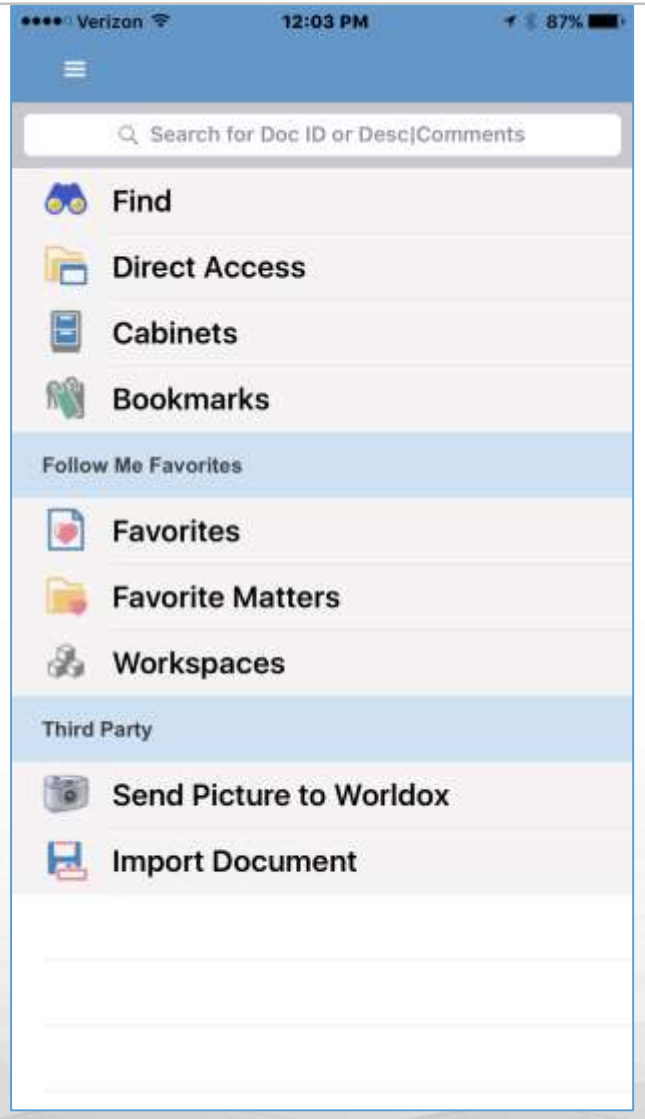
Linked Devices

These devices are currently linked to your Workshare account.

Last Activity	Country	First Name	Last Name	Email	Device Name	Registered Date	
28 minutes ago	United Kingdom	Vera	Khromova	vera.khromova@workshare.com	ln1-vera-01	about an hour ago	Unlink
about a minute ago	United Kingdom	Chris	Phillips	chris.phillips@workshare.com	ln1-chrisp-02	about 5 hours ago	Unlink
less than a minute ago	United Kingdom	Christine	Davies	christine.davies@workshare.com	ln1-hillman.workshare.com	about 5 hours ago	Unlink
3 minutes ago	United Kingdom	Helen	Sagal	helen.sagal@workshare.com	LN1-HELENS-05	about 5 hours ago	Unlink
less than a minute ago	United Kingdom	Mei	Tan	mei.tan@workshare.com	ln1-whit-10.wor LN1-HELENS-05	bout 5 hours ago	Unlink
about an hour ago	United States	George	Lavallee	George.Lavallee@workshare.com	Workshare Desktop	about 9 hours ago	Unlink
less than a minute ago	United Kingdom	Sara	Abed	sara.abed@workshare.com	ln1-sara-01	about 22 hours ago	Unlink
2 minutes ago	United States	Peter	Concannon	peter.concannon@workshare.com	PeterC-T430U	about 22 hours ago	Unlink

Mobile Access





Any Questions?

For more information:
https://www.worldox.com/security/