Cyber Security
Education and Planning
June 27, 2017 / Boston, MA
Why isn’t everyone prioritizing Security?
What are the top 3 issues or annoyances within your firm?

1. Security/Risk Management
2. Change: Managing Expectations (Users and Management)
3. Change: Users' Acceptance of Change
4. Email Management
5. Change: Keeping Up with New Versions of Software
6. Training: Meeting Needs for and/or Getting Participation in Training

Trending data 2015-2012
Learning the Hard Way

In the news...

<table>
<thead>
<tr>
<th>Company</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>110 million individual’s contact information stolen</td>
</tr>
<tr>
<td>Neiman Marcus</td>
<td>350,000 individual’s credit card information stolen</td>
</tr>
<tr>
<td>Michaels</td>
<td>2.6 million individual’s credit card information stolen</td>
</tr>
<tr>
<td>Yahoo</td>
<td>Email service for 1 billion users hacked</td>
</tr>
<tr>
<td>aaronbrothers</td>
<td>400,000 credit and debit cards were compromised</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Hacked from within for two weeks</td>
</tr>
<tr>
<td>eBay</td>
<td>Cyber attack led to access of 223 million user accounts</td>
</tr>
<tr>
<td>Feedly</td>
<td>15 million users affected by denial-of-service attacks</td>
</tr>
<tr>
<td>Supervalu</td>
<td>Personal data from multiple locations compromised</td>
</tr>
<tr>
<td>EVERNOTE</td>
<td>100 million users affected by denial-of-service attacks</td>
</tr>
<tr>
<td>Evernote</td>
<td>Hacked from within for two weeks</td>
</tr>
<tr>
<td>PF Chang’s</td>
<td>Credit card information for 33 locations was stolen</td>
</tr>
<tr>
<td>UPS</td>
<td>100 million customers affected by denial-of-service attacks</td>
</tr>
<tr>
<td>The Home Depot</td>
<td>56 million shoppers credit card information stolen</td>
</tr>
<tr>
<td>Google</td>
<td>5 million Gmail username and passwords stolen</td>
</tr>
<tr>
<td>iCloud</td>
<td>Online data storage hacked to post celebrities’ private photos online</td>
</tr>
<tr>
<td>CHS Community Health Systems, Inc.</td>
<td>Personal data for 4.5 million patients compromised</td>
</tr>
<tr>
<td>Supervalu</td>
<td>Personal data from multiple locations compromised</td>
</tr>
<tr>
<td>mossack fonseca</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
FBI Warnings to Law Firms

FBI Alert Warns of Criminals Seeking Access to Law Firm Networks
March 11, 2016

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

Cyber Security Planning
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).
III. SECURITY PROGRAM—FRAMEWORKS AND STANDARDS

- 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
- 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
<table>
<thead>
<tr>
<th>Current</th>
<th>Planned</th>
<th>Proactive</th>
</tr>
</thead>
</table>
| • 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

In your opinion, what is the greatest information security threat your organization faces today?

- External bad actor threats (hackers, etc): 11.9%
- Internal bad actor threats (malicious employees/contractors, etc): 9.9%
- Mobile devices: 6.6%
- Malware: 5.3%
- Unauthorized data leakage: 2.6%
- Cloud computing: 0.7%
- Unpatched software/devices: 0.7%
- Third party providers: 0.7%
- Other (please specify): 13%

80.9%
Risk Assessment

- Content
- Context
- Control

DMS

Cyber Security Planning
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

Matter based

Document type based

- Vital
- Important
- Useful
- Non-essential

Cyber Security Planning

15
Software Updates

Windows / Office Updates

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
• **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.
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)

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

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 seller's business location.
Least Privilege
Unique User Accounts
Remote Content Access
Bring Your Own Device (BYOD)
What about paper?

Scanning to DMS from MFD
Scanning to DMS from personal device
Sony Digital Paper
Securing Paper

- Security layers ARE ignored! Why?
- If it’s not easy to use it simply won’t be!
- The medium of paper is preferred for essential legal workflow.
Intrusion Detection Services

$4000 + monthly
Dedicated Devices and 24/7 Staffing

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Starting Price, USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Network</td>
<td>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.</td>
<td>$3,000</td>
</tr>
<tr>
<td>Internal Network</td>
<td>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.</td>
<td>$4,000</td>
</tr>
<tr>
<td>Web Application</td>
<td>Price is for a single web application penetration test, in conjunction with an external or internal network penetration test.</td>
<td>$1,200</td>
</tr>
<tr>
<td>Wireless</td>
<td>Price is for a wireless penetration test, in conjunction with an internal network penetration test, for one wireless access point and associated client devices.</td>
<td>$3,000</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Price is for a Remote social engineering test, including two separate electronic attack vectors including spear phishing email Engineering directed at human targets within your organization, in conjunction with an external network penetration test.</td>
<td>$3,000</td>
</tr>
</tbody>
</table>

http://highbitsecurity.com
Encryption
Encryption Options

Full Disk

- Totaled up, the costs of FDE work out at $232 per user, per year (zdnet)
- Ponemon found that the cost of FDE on laptop and desktop computers in the U.S. per year was $235 (networkcomputing.com)

Container

Line of Business Software
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

2-Way Collaboration
- Version Control
- Process History Saved in Audit Trail

Secure Sharing
- DRM
- Metadata Removal

Mobility
- Browser
- Mobile Device

Personal File Sync
- Remote Data Wipe

Worldox Encryption At Rest
- Background encryption on the fly, transparent to users
- File level encryption using the AES standard
- Firm controlled encryption keys
- Secondary encryption key for super sensitive files
Worldox Encryption At Rest

Multi-Tiered Encryption Technology

- Encrypts data at rest on servers and file shares
- Employs encryption at the Application, Database and File System layers.
- Combine it with AD Integration, Ethical Walls and a least privilege philosophy to reduce vulnerability even further.
- Site Certificate – general overall safety of Worldox data
- User / Machine Certificate – specific safety over rogue users, lost passwords
- Worldox Admin Lockout
Secure Sharing
Secure Collaboration

Cyber Security Planning
Secure Collaboration

Cyber Security Planning

2014 RESELLER AGREEMENT

WSC INC.

ARTICLE I PARTIES TO THIS AGREEMENT

This Agreement is made by and between:

WSC Inc.

W3C, Inc.

3850 Nobel Dr.

San Diego, CA 92121

and

ABC, Inc.

2901 University Blvd.

Suite 305

Glen Rock, NJ 07452

(hereinafter referred to as "WSC")

(hereinafter referred to as the "Reseller")

ARTICLE II PREMISES OF THIS AGREEMENT

WHEREAS, WSC is engaged in the sale and licensing of computer software throughout the United States of various electronic products, related accessories and software; and

WHEREAS, the Reseller desires to sell or license such products, accessories and software and represents that it is capable of promoting the necessary business therein.

NOW THEREFORE, by reason of the foregoing premises and in consideration of the mutual covenants hereinafter set forth, the parties agree as follows:

ARTICLE II THE TERM AND DEFINITIONS

b) Term: This Agreement shall commence as of the Effective Date and expire on March 31, 2015, unless terminated in accordance with Article IV, Section 10.0.

b) Products: The term the "Products" relates to those products, accessories and software of Display which the Reseller is authorized to purchase and sell or license pursuant to each Schedule.

b) Schedules: Each Schedule identifies the Products which the Reseller is authorized to purchase and sell or license, and contains terms and conditions regarding the Products which may be subject to or different from the General Terms and conditions set forth in Article IV.

b) General Definitions:

The term "Principal Business Location" refers to the Reseller’s address set forth in Article I.

The term "Authorized Business Location" refers to the Principal Business Location and to the locations which are identified as Authorized Business Locations, if any, listed below.
## Mobile Content Management

### All Devices

These devices are currently linked to your Workshare account.

<table>
<thead>
<tr>
<th>Last Activity</th>
<th>Country</th>
<th>First Name</th>
<th>Last Name</th>
<th>Email</th>
<th>Device Name</th>
<th>Registered Date</th>
<th>Unlink</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 minutes ago</td>
<td>United Kingdom</td>
<td>Vera</td>
<td>Khromova</td>
<td><a href="mailto:vera.khromova@workshare.com">vera.khromova@workshare.com</a></td>
<td>In1-vera-01</td>
<td>about an hour ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>about a minute ago</td>
<td>United Kingdom</td>
<td>Chris</td>
<td>Phillips</td>
<td><a href="mailto:chris.phillips@workshare.com">chris.phillips@workshare.com</a></td>
<td>In1-chrisp-02</td>
<td>about 5 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>less than a minute ago</td>
<td>United Kingdom</td>
<td>Christine</td>
<td>Davies</td>
<td><a href="mailto:christine.davies@workshare.com">christine.davies@workshare.com</a></td>
<td>In1-hillman.workshare.com</td>
<td>about 5 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>3 minutes ago</td>
<td>United Kingdom</td>
<td>Helen</td>
<td>Sagal</td>
<td><a href="mailto:helen.sagal@workshare.com">helen.sagal@workshare.com</a></td>
<td>LN1-HELENS-05</td>
<td>about 5 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>less than a minute ago</td>
<td>United Kingdom</td>
<td>Mei</td>
<td>Tan</td>
<td><a href="mailto:mei.tan@workshare.com">mei.tan@workshare.com</a></td>
<td>In1-whil-10 work LN1-HELENS-05</td>
<td>about 5 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>about an hour ago</td>
<td>United States</td>
<td>George</td>
<td>Lavallee</td>
<td><a href="mailto:George.Lavallee@workshare.com">George.Lavallee@workshare.com</a></td>
<td>Workshare Desktop</td>
<td>about 9 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>less than a minute ago</td>
<td>United Kingdom</td>
<td>Sara</td>
<td>Abed</td>
<td><a href="mailto:sara.abed@workshare.com">sara.abed@workshare.com</a></td>
<td>In1-sara-01</td>
<td>about 22 hours ago</td>
<td>Unlink</td>
</tr>
<tr>
<td>2 minutes ago</td>
<td>United States</td>
<td>Peter</td>
<td>Concannon</td>
<td><a href="mailto:peter.concannon@workshare.com">peter.concannon@workshare.com</a></td>
<td>PeterC-T430U</td>
<td>about 22 hours ago</td>
<td>Unlink</td>
</tr>
</tbody>
</table>
Mobile Access

Cyber Security Planning
Protect Yourself & Your Firm

- Are Microsoft updates installed on all servers and user PCs in a timely manner?
- Are all users required to have complex passwords and change them periodically?
- Does your firm utilize dual-factor authentication?
- Are any user accounts Domain Admins?
- Do any users (IT included) have full administrator permissions to local PCs?
- Are IT Dept members included in Ethical Walls other than those within which they need to see the documents to do their jobs?
- Are users allowed to delete documents?
- Are users allowed to connect external media to their PCs? (USB drives)

- Are users allowed to use their own laptops and other mobile devices?
- Are workstations, laptops and other mobile devices encrypted?
- Does your firm have policies outlining approved secure methods for sharing files?
- When people leave the firm, are there policies and procedures in place for decommissioning their accounts?
- Does your firm have a mandatory security awareness educational program?
- Does your firm have a cyber-insurance policy?
Worldox/DMS tips

- Have you upgraded to our current code release?
- Does WDAdmin have a complex password?
- Are there WDAdmin accounts that are also Domain Admins?
- How many people are Worldox Managers?
- Has Active Directory Integration been deployed?
- Are document retention policies set up?
- Are confidential documents protected using Cabinet restrictions or ethical walls?
- Are UNC paths used to access Worldox Cabinets?
- Are users who no longer work for the firm or require access to Worldox still enabled on the system?
- Are security groups used to allow quick and easy document security settings?
- How are files within Worldox accessed remotely or shared externally?
Harden Your Defenses

1) Spam filters
2) Encryption
3) Off-site backups
4) Remote Access Policy
5) Patching servers and workstations
6) Firewalls
7) Virtual Private Network (VPN)
8) Group Policies
9) WSUS or some other patching product
10) Network Access Control (NAC)
11) Vulnerability scanning
12) Mobile device management
13) Security Information & Event Management (SIEM)
Any Questions?

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