Three Growing Trends that can weaken Data Security

- Legislative websites are targets
- Increase in BYOD – IT professionals cannot stop 100% “oopsie” clicks done by users; or lost and stolen devices
- Increase in Cloud platforms
  - Are they safe?
  - Where is your data?
  - Do you have control over its maintenance and retention?
  - Can you comply with all laws and policies of your legislature?

Open Records initiatives
  - Increase in demand for transparency / records requests
  - How do the Cloud and BYOD impact Open Records requirements?
TREND 1: INCREASE IN THREATS, THE HUMAN FACTOR AND BYOD

SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.
DATA IS INCREASINGLY AVAILABLE

- 75% of security leaders expect their cloud security budget to increase dramatically over the next 3-5 years.
- 86% of security leaders surveyed say their organizations are now moving to the cloud.
- 44% of security leaders said that they expect a major cloud provider to suffer a significant security breach in the future.

Learn more at IBM.com/security/cloud
THREATS OCCUR INCREASINGLY OFTEN

- In May it was reported that 230,000 new malware attacks are being launched every day
- 27% of all recorded malware first appeared in 2015
- In the US, cyber crime costs an estimated $15.42 million dollars a year
- 600,000 Facebook accounts are hacked every day
- Between Java, Adobe reader and Flash, 99% of all computers are vulnerable to exploits
- The average number of successful attacks per week is now around 138, compared to 50 just 5 years ago
RECONCILING IDEAS OF SECURITY
HUMAN FACTOR

Security software: perception vs. reality
Percent; n = 378

- **Antivirus**
  - Claim to have software installed: 87%
  - Actually have software installed: 94%

- **Antispyware**
  - Claim to have software installed: 70%
  - Actually have software installed: 55%

- **Firewall**
  - Claim to have software installed: 73%
  - Actually have software installed: 81%

- **Antispam**
  - Claim to have software installed: 61%
  - Actually have software installed: 21%

- **Antiphishing**
  - Claim to have software installed: 27%
  - Actually have software installed: 12%

- Only 51% of those with AV software had DAT files updated within the last week.
- Only 64% of those with firewalls actually had them enabled.
TRAINING - PASSWORDS

Password security – how to get secure passwords, that people can remember (i.e. that won’t end up on sticky notes)

**Dig if you will the picture! ’95 high five**

D1wtp!’95#^5

**I hate changing my stupid password all the time**

%1Hcm5p4tt010116%

**The rain in Spain falls mainly on the plain**

Tr15fm0tp!063016
TRAINING - PHISHING

- Only follow links you receive from trusted sources
  - Even if it is a trusted source, does the link make sense???

- Very few reputable companies will ask you to conduct business by clicking a link in an email.
  - If you think it is legitimate, still don’t click it, go to the companies web page and find a link there.
Box login from "Windows Internet Explorer"

This application has now been added to your login activity list. If this was you, you can disregard this email.

- **Application:** Windows Internet Explorer
- **Time:** Thursday, July 7, 2016 at 12:25:08 PM MST
- **Location:** Meridian, ID, USA (Approximated from IP address 164.165.0.0)

You can manage your login activity list from the **Security** tab and your notifications from the **Notifications** tab of your Account Settings.

If you did not add this application, click the button below to remove it from your login activity list.

[Remove Application]
SECURITY BEST PRACTICES

- Ability to remotely wipe (factory reset) mobile devices that are connected to Exchange.
- Ability to require devices to have a pass-code for access.
- Personal devices of legislators and staff on network segment separate from data / Separate internal trusted users from public access users.
- Audit reports on software loaded on machines, check for vulnerabilities, available updates, etc.
- Password policy (e.g. different for users with admin privileges)
- While database driven, our website does not touch our DB.
MALWARE ATTACKS VIA TRUSTED 3RD PARTY VENDORS ALSO A RISK

How do 3rd party vendors support your organization?

Same best practices should apply!
TREND 2 – INCREASE IN CLOUD SERVICES

Cloud Service Layers:

SaaS - Software as a service
- Any off the shelf application accessed via the web (Google, Facebook, Twitter)

PaaS – Platform as a Service
- Development environment for web applications

IaaS – Infrastructure as a Service
- Virtualized hardware to build an infrastructure across the internet – via Public, Private and Hybrid Clouds
BENEFITS: LEVERAGE CLOUD SERVICES TO YOUR ADVANTAGE / MINIMIZE THE RISKS

• Cost savings – economies of scale
• IT staff work more strategically – don’t need to manage servers
• Scalable resources readily available
• Capacity planning far more flexible
• Only pay for the actual services utilized
• Insulated from physical hardware failures
• Leave high-end security / infrastructure work to the experts
CLOUD SERVICES: WHAT ARE THE RISKS?

- The physical server is no longer behind your ‘lock and key’
- Is data private and secure
- Will information be available in the event of an Open Records request
- What if you lose Internet connectivity
- What about Disaster Recovery – is redundancy built into your hosted applications
- What are your vendor’s dependencies (i.e. PaaS vendors likely running on a IaaS platform such as Amazon, Azure or Google
SNAPSHOT OF VIRGINIA CLOUD SOLUTIONS

- Entire Legislature utilizes cloud services for email -- either Google's Gmail or Microsoft's Office365
- Amazon S3 Storage services used for hosting array of legislative publications
- Development environment for a number of cloud applications
  - House Members
  - Interim Studies
  - Publications
  - Chamber and Committee agendas (public and private components)
CASE STUDIES IN IDAHO: BOX.COM DATA STORAGE

- Primary file storage for legislators
  - Data saved to “My Documents” location synced by Box.com app. to cloud.

- Collaborative file shares for various groups
  - Committees
  - Caucuses
  - Various staff sections

- Community file share
  - Training documents
  - Policy/procedure
  - Collateral (e.g. “how a bill becomes a law” document)

- File sharing
  - Groups of files (e.g. issue related)
  - Individual files (e.g. something too big for email)
WHY BOX.COM
ADVANTAGES OVER COMPETITORS

- Granular access control and permissions
  - Down line control of shared files to prevent data leakage
  - How long shared links are available
  - Can limit a share within the network
  - Folder by folder and doc by doc permissions
  - Control over the number of devices per user

- AD integration
  - Deleting an account on AD can automatically delete the associated directories/files
  - Single signon

- Backend reporting
  - See what files have been shared by who, with who
  - Volume of shares and access to those shares
GOVDELIVERY MASS MAILING SERVICE

- Template driven, professional looking mass emailing’s
- Mailing list management
- CAN-SPAM “compliance” (AKA the meat and potatoes)
- Required some policy/procedure development
  - Should not contain campaign or partisan material
  - We don’t use the feature that allows posting directly to social networks
CONSIDERATIONS WHEN MOVING TO THE CLOUD

- Know who you are dealing with

- Service Level Agreements - cover a range of service limits and guidelines around performance, privacy, availability, costs and more (i.e., guaranteed uptime?)

- Transparency of Quality of Service Delivery
  - How are service outages reported?
  - Are audit reports available
  - Is data backed up
CONSIDERATIONS WHEN MOVING TO THE CLOUD

Support
- When are technicians ‘on the job’ (hopefully 24/7)

What tools are available
- For application development – do you need PHP or .NET support; SQL Server or MySQL?

- For online storage and Cloud email – do you need e-discovery tools?

- Can vendor comply with your retention policies?

Security – Cloud Vendor’s Responsibility
- How does vendor assess security
- What security standards do they meet?
- Are data centers redundant?
Security – When you move to the Cloud - your responsibility does not diminish – do your research!

Make sure to ask -- Who owns your data and what can the cloud provider do with it?

Penetration testing / Intrusion detection – conduct your own audits on your hosted applications (PaaS)

Lots of security companies to assist with this

Know your retention policies – how will Cloud vendor meet them

How are data backups handled

In the event of Disaster Recovery / or db corruption – how fast can you get your backups

How long is information stored
CLOUD DATA SECURITY CONSIDERATIONS

- Division of liability for data breach is likely governed by contract
  - Be wary of provider’s “standard” or click-through terms of service
  - Pay close attention to indemnification provisions (can shift risk to provider or to you)

- Can you audit provider’s security measures?

- Is provider required to immediately notify you if your data is stolen from their platform?

TREND 3: IMPACT OF RECORDS RETENTION AND OPEN RECORDS POLICIES
Legal duty to preserve certain records for a prescribed amount of time

Highly state-specific

Records retention schedule
  - Typically approved by state archives (or another designated agency or official)
  - Prescribes minimum retention periods for certain classes of documents
Under Texas House and Senate records retention schedules, an email can be:

- **Transitory Information** – retain until purpose of record has been fulfilled
- **General Correspondence** – retain 2 years
- **Administrative Correspondence** – retain 4 years, then State Archivist must review before destruction
- **Legislative Working Files** – retain forever
TSLAC RECOMMENDS YOU FILE YOUR EMAIL LIKE THIS . . .

https://www.tsl.texas.gov/slrm/blog/2016/03/faq-how-can-i-set-up-an-email-filing-system/
THE CLOUD WAS MADE FOR RETENTION

- “Any state record may be created or stored electronically . . . .” (Tex. Gov’t Code Sec. 441.189(a).)
- Cloud storage benefits
  - Vast and inexpensive storage
  - Enterprise data centers
  - Extensive backups
- The new Texas Digital Archive is stored on Amazon Web Services GovCloud

- Receives one too many L.L.Bean advertisements and deletes the entire Gmail account?
- Configures POP3 to delete Hotmails from the server when downloaded to a smartphone?
- Leaves the legislature without providing a copy of the Dropbox files?
- Quits paying for extra iTunes storage?
Cloud storage could be a very safe and efficient place to retain records.

Regardless of the system used, records retention compliance calls for active involvement by trained staff.

Unless the rules are simplified, it’s probably impossible to fully automate records retention.
Legal duty to make certain information available to the public for inspection and copying

Every state has one

Applies to the legislative branch, to some extent, in at least 42 states

This presentation addresses only technology issues related to open records

It depends on your state’s law, but it may not matter.

Texas law: “The definition of ‘public information’ . . . applies to and includes any electronic communication created, transmitted, received, or maintained on any device if the communication is in connection with the transaction of official business.” (Tex. Gov’t Code Sec. 552.002(a-2).)
WHAT IF I GOVERN USING ONLY SNAPCHAT AND INSTAGRAM?

- Ask your favorite Legislative Council attorney, but someone may have thought of that.

- Texas law: “The general forms in which the media containing public information exist include a book, paper, letter, document, e-mail, Internet posting, text message, instant message, other electronic communication, printout, photograph, film, tape, microfiche, microfilm, photostat, sound recording, map, and drawing and a voice, data, or video representation held in computer memory.” (Tex. Gov’t Code Sec. 552.002(c).)
WHAT IF I.T. GETS A REQUEST FOR A MEMBER’S EMAILS?

- In Texas, an open records request must be submitted to the governmental body with legal custody of the requested information.

- Texas AG ruled that Texas Legislative Council does not have legal custody of emails sent or received by legislators, committees, and other legislative agencies and did not have to provide those emails. (Open Records Letter No. OR2004-5690 (2004).)
COMPELLED ACCESS TO CLOUD DATA
CONSIDERATIONS

- You have more knowledge and control over what happens to data in your own data center
- OTOH, disclosing user data is bad for a cloud provider’s business and it has more money than your state does to fight disclosure
  - See MS Ireland case & Apple San Bernardino case
So what does all of this mean??????

The Sky is not Falling!!!!

- Be proactive!
- Move forward – cautiously informed.
- Do your own security audits.
- Know who you are dealing with.
- Know your policies and laws.
- Don’t ask IF – ask WHEN
Resources

• **http://Digitalattackmap.com** – Shows current threats (similar, but cooler effects: **http://hp.ipviking.com/**)

• **https://zeltser.com/lookup-malicious-websites/** - Free tools for checking malicious websites

• **http://www.file-extensions.org/filetype/extension/name/dangerous-malicious-files** - Shows common potentially dangerous file extensions.

• **http://mxtoolbox.com/blacklists.aspx** - Check your mail server against email blacklists
More Resources - Data Breach Laws

• State laws
  • 47 states, DC, Guam, Puerto Rico, Virgin Islands
  • Some state’s laws apply to governmental entities
  • Notifications, fines, lawsuits, credit monitoring

• Federal law (HIPAA, FERPA, SEC, FTC, DOJ, etc.)
Excellent multistate survey of open records laws in the digital age:

Google Law Enforcement Requests
July – December, 2015

• 12,523 requests
• 27,157 user accounts
• 79% of requests – some data produced

https://www.google.com/transparencyreport/userdatarequests/US/
Apple Law Enforcement Requests
July – December, 2015

- Account requests
  - 1,015 requests
  - 5,192 user accounts
  - 82% of requests – some data produced

- Device requests
  - 4,000 requests
  - 16,112 devices
  - 80% of requests – some data produced

Microsoft Law Enforcement Requests
July – December, 2015

United States

Requests
Total number of requests
5,297
Accounts/users specified in request
12,355

Disclosures
% Disclosed content
21.00%
% Only subscriber/transactional data
15.07%
% No data found
9.49%
% Rejected
54.36%

https://www.microsoft.com/about/csr/transparencyhub/lerr/
## SCA Law Enforcement Requests

<table>
<thead>
<tr>
<th>Request Type</th>
<th>Information Subject to Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subpoena without notice</td>
<td>Non-content</td>
</tr>
<tr>
<td>Subpoena with notice</td>
<td>Content</td>
</tr>
<tr>
<td>Court order without notice</td>
<td>Non-content</td>
</tr>
<tr>
<td>Court order with notice</td>
<td>Content</td>
</tr>
<tr>
<td>Search warrant (without notice)</td>
<td>Content</td>
</tr>
</tbody>
</table>

Microsoft Ireland Case

- MSN.com email account stored on servers in Dublin, Ireland
- Dec. 2013: Stored Communications Act search warrant:
  - (a) “The contents of all e-mails stored in the account, including copies of e-mails sent from the account”;
  - (b) “All records or other information regarding the identification of the account,” including, among other things, the name, physical address, telephone numbers, session times and durations, log-in IP addresses, and sources of payment associated with the account;
  - (c) “All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files”; and
  - (d) “All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken.”

MS Ireland Case, cont’d

- July 2016: Second Circuit Court of Appeals held that Congress intended SCA to apply only in the United States because Congress didn’t say otherwise
- Result: in NY, CT, and VT, an SCA search warrant does not apply to data stored outside of the United States
What We Know

• Application of Stored Communications Act to cloud service providers is unsettled and evolving

• Privacy policy, terms of service, and contract are the best tools available to protect data
  • Without them, providers may voluntarily disclose customer data in certain circumstances

• Providers must disclose user data in criminal investigations

• Providers generally prohibited from disclosing user data in response to civil subpoenas*

* See, e.g., In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 609 (E.D. Va. 2008) (holding that a civil discovery subpoena is not an exception to the SCA that would allow an ISP to disclose emails).
To the disappointment of the Forty Thieves, their leader had forgotten the password again.